THE PRIME DISCRIMINANT FACTORIZATION OF DISCRIMINANTS OF ALGEBRAIC NUMBER FIELDS

BY

DANNY NEVIN DAVIS

A DISSERTATION PRESENTED TO THE GRADUATE COUNCIL OF
THE UNIVERSITY OF FLORIDA
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

1978

Dedicated to

my parents,

Nevin B. and Frances L. Davis

ACKNOWLEDGMENTS

The author wishes to express his appreciation to Robert Long for his years of instruction and encouragement in the attainment of this degree; he is owed a particular debt of graditude for his efforts --too numerous to mention-- in connection with this dissertation.

Shorter College has generously provided xeroxing services, a typewriter and various other encouragements. In this regard, the author especially thanks Dr. Randall Minor, Tom Lagow and Bob Chisholm.

The author also acknowledges his indebtedness to his wife, Jenny; she typed the dissertation; she advised, planned and edited; but, mostly, she went the many miles between then and now with the constancy that got us through.

TABLE OF CONTENTS

		Page
Acknowledgments		iii
List of Symbols		v
Abstract		viii
Section I	BASIC CONCEPTS AND TERMINOLOGY	1
Section II	UNIQUENESS IN THE FACTORIZATION AND THE CLASSICAL RESULT	7
Section III	DIRECTIONS FOR GENERALIZATIONS	10
Section IV	THE FIRST GENERALIZATION	11
Section V	THE CASE OF QUADRATIC DISCRIMINANT IDEALS	20
Section VI	THE CASE OF QUADRATIC IDELE DISCRIMINANTS	34
Section VII	REMARKS ON A THEOREM OF GOLDSTEIN	44
Section VIII	THE CASE OF CYCLIC ℓ-DISCRIMINANT IDEALS, $\ell > 2$	47
Bibliography		57
Biographical Sketch		58

LIST OF SYMBOLS

K, L	algebraic number fields
A, B	rings of integers of K, L respectively
U, V	unit groups of K, L respectively
U_{p^m}	$\{u \in U: u \equiv 1 \bmod p^m\}$
U_{v_∞}	totally positive units of K
K_p	completion of K at the prime ideal p
K_v	completion of K at prime v (used for both finite and infinite primes)
$\hat{A}_p$	ring of integers of K_p
$\hat{U}_p$	unit group of K_p
U_v	unit group of K_v
$\hat{U}_p(m)$	$\{u \in \hat{U}_p: u \equiv 1 \bmod (p\hat{A}_p)^m\}$
J_K	ideles of K
U_K	unit ideles of K
E_c	maximal abelian extension of K with conductor dividing the cycle c
$a \mid b$	a divides b
C_m	cyclotomic field of m^{th} roots of 1
$d_{L/K}$	numerical discriminant of L/K (in case B is free as an A-module)
$\mathcal{D}_{L/K}$	idele discriminant of L/K
$D_{L/K}$	discriminant ideal of L/K
$d_{L\otimes K_p}$	discriminant of any basis of $B\otimes_A \hat{A}_p$ as an $\hat{A}_p$-module considered mod $\hat{U}_p^2$

$d'_{L/K}$	discriminant of any basis of L/K considered mod K^{*2}
$e(\mathfrak{b}/K)$	ramification index of $\mathfrak{b}$ over K ($\mathfrak{b}$ is a prime ideal in some extension of K)
$e(\hat{L}/\hat{K})$	ramification index of the prime in a p-adic field $\hat{L}$ over the p-adic field $\hat{K}$
$f(\mathfrak{b}/K)$	inertial degree of $\mathfrak{b}$ over K ($\mathfrak{b}$ is a prime ideal in some extension of K)
$f(\hat{L}/\hat{K})$	inertial degree of the prime in a p-adic field $\hat{L}$ over the p-adic field $\hat{K}$
$F_{L/K}$	conductor of an extension L/K
$\|G\|$	order of a finite group G
$(G)_\ell$	ℓ-group component of an abelian group G
h_K^+	$[K^+:K]$, the narrow class number of K
h_K	order of the (ideal) class group of K
I_K, I	group of fractional ideals of K
P_K, P	group of principal fractional ideals of K
$K^{(1)}$	Hilbert class field of K
K^+	extended Hilbert class field of K
$N(\mathfrak{p})$, $N_{K/Q}(\mathfrak{p})$	the order of $A/\mathfrak{p}$
N, $N_{K/Q}$	absolute norm
$N_{L/K}$	norm from L to K
Q	rational field
$\sigma(\ell)$	cyclic group of order ℓ
$Tr_{L/K}$	trace from L to K
$\nu_{\mathfrak{p}}(a)$, $\nu_{\mathfrak{p}}(a)$	power of the prime ideal $\mathfrak{p}$ in the ideal a or (a), respectively
ν_∞	formal product of all real primes

Z	rational integers
ζ_m	primitive m^{th} root of 1
$[[\cdot]]$	greatest integer function
$<a>$	cyclic group generated by a
$W_c(v)$	an open neighborhood about 1 in $K_v^{\cdot}$ (see p. 14)

Abstract of Dissertation Presented to the Graduate Council
of the University of Florida in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

THE PRIME DISCRIMINANT FACTORIZATION OF DISCRIMINANTS OF ALGEBRAIC NUMBER FIELDS

By

Danny Nevin Davis

December 1978

Chairman: Mark L. Teply
Major Department: Mathematics

Let $Q(\sqrt{d})$ be a quadratic extension of the rationals with discriminant d. In this case d is called a quadratic discriminant in Q (or, an absolute quadratic discriminant); moreover, d is called a prime quadratic discriminant in Q whenever d is divisible by exactly one rational prime. It is a well known result in algebraic number theory that, in Q, every quadratic discriminant can be factored uniquely as a product of prime quadratic discriminants. In this dissertation several generalizations of this classical result are proved.

The first step toward these generalizations is that of extending to the discriminant ideal the concept of prime discriminant. Let K be an algebraic number field. Call the discriminant ideal of any quadratic extension of K a quadratic discriminant ideal in K. It is proved that any quadratic discriminant ideal in K can be factored uniquely as a product of prime quadratic discriminant ideals if and only if K is totally real with odd narrow class number.

The concept of prime discriminant is then further extended to a relatively new discriminant due to A. Fröhlich which is here called the idele discriminant. This discriminant is defined for any L/K to be a certain class of the ideles of K modulo the squares of the unit ideles. The idele discriminant is paramount among discriminants because while possessing the universal applicability of the discriminant ideal it does not lose the numerical specificality of the absolute discriminant. In particular, when the base field is Q the idele discriminant is effectively an absolute discriminant. Therefore, a direct generalization of the classical result is achieved when it is proved that the aforementioned result concerning the factorization of discriminant ideals holds as well for idele discriminants.

Besides extending the concept of prime discriminant, one additional direction for the generalization of the classical result is pursued. In the factorization theorems mentioned thus far the discriminants were generated in a fixed base field K by quadratic extensions of K. An investigation is begun here into the possibility of generating the discriminants from extensions over K with fixed Galois group other than cyclic of order 2. The only case considered is that in which the Galois group is cyclic of odd prime order. Let ℓ be an odd prime. It is proved, for example, that if K is an imaginary quadratic field with class number prime to ℓ and if K is not the cyclotomic field of ℓ^{th} roots of unity, then any discriminant ideal of K that is generated by a cyclic ℓ-extension of K has a unique factorization as a product of prime discriminant ideals likewise generated.

SECTION I
BASIC CONCEPTS AND TERMINOLOGY

An algebraic number field is any finite extension of the rational number field Q. Of utmost significance to the study of algebraic number fields is the concept of integer in these fields. The ring of integers of an algebraic number field K is the integral closure of Z, the rational integers, in K.

In general the ring of integers of an algebraic number field is not a unique factorization domain. For example, the ring of integers of $Q(\sqrt{-5})$ is $Z[\sqrt{-5}]$ but $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$, where all four factors are irreducible elements in $Z[\sqrt{-5}]$. (For more details see [9, pp. 49-54].) Fortunately, however, the ring of integers of any algebraic number field is a Dedekind domain. We shall now list the important properties this fact insures for the ring of integers A of an arbitrary number field K.

1) Every prime ideal of A has an inverse in the monoid of fractional ideals of A. (A fractional ideal of A is an A-submodule I of K for which there exists an integer $d \in A - \{0\}$ such that $dI \subseteq A$.)

2) Every (nonzero) fractional ideal of A has a unique factorization as a product of powers of prime ideals of A.

3) The monoid of nonzero fractional ideals of A is a group.

Throughout this thesis the symbols K and L will stand for algebraic number fields. The rings of integers of K and L are denoted by A and B, respectively, and the groups of units of A and B are

denoted by U and V, respectively. We refer to U (respectively V) as the units of K (respectively L).

Let $\{x_1,\ldots,x_n\}$ be a basis for an extension L/K. The discriminant of this basis is defined by the relation $d_{L/K}(x_1,\ldots,x_n) = \det(tr_{L/K}(x_ix_j))$, where $tr_{L/K}$ stands for the trace from L to K. The discriminant ideal of L/K, denoted by $D_{L/K}$, is the ideal of K (i.e.,A) generated by the numbers $d_{L/K}(x_1,\ldots,x_n)$ as $\{x_1,\ldots,x_n\}$ ranges over all bases of L/K with $x_i \in B$ for all i. Perhaps the most important property of the discriminant ideal of L/K is that a prime ideal p of K (called a prime K-ideal) divides $D_{L/K}$ if and only if p ramifies in L, i.e., there is a prime L-ideal b such that the power of b dividing pB is greater than 1. An interesting consequence of this property of $D_{L/K}$ is that only a finite number of prime K-ideals ramify in L. Finding the exact factorization of pB, for any prime K-ideal p, as a product of prime L-ideals is an important problem in "ramification theory" and the discriminant ideal plays a large role in this part of algebraic number theory.

Let $pB = \prod_{i=1}^{g} b_i^{e_i}$ be the prime L-ideal factorization of the prime K-ideal p. The positive integer e_i is called the index of ramification of b_i over K and is denoted $e(b_i/K)$. The index of finite fields $[B/b_i: A/p]$ is called the degree of inertia of b_i over K and is denoted $f(b_i/K)$.

The following identity is perhaps the central theorem of ramification theory : $\sum_{i=1}^{g} e(b_i/K)f(b_i/K) = [L:K]$. (For a proof see [9, p. 71].) This very useful result will be applied frequently throughout the thesis often without specific reference to the general identity.

We shall say that the primes b_i are the prime L-ideals that lie above p; it is, in fact, the case that $b_i \cap A = p$ for all i and these are the only prime L-ideals with this property.

The symbol $N(p)$, called the absolute norm of p, is used to denote $|A/p|$ and this definition extends to $N(a)$ for any fractional K-ideal by multiplicitivity using the properties of Dedekind domain listed above. $N(a)$ is called the absolute norm of the ideal a and is related to the absolute norm map $N_{K/Q}: K^* \to Q^*$ by $N(aA) = \pm N_{K/Q}(a)$ for all $a \in K^*$. (We will always use R^* to denote the group of units of a commutative ring R which has a multiplicative identity.)

A frequently encountered class of extension L/K is that in which B is free as an A-module. In this case, a basis for B as an A-module is called a relative integral basis of L/K and the discriminant of a relative integral basis of L/K is called a relative discriminant of L/K. When we speak of the relative integral basis or relative discriminant of an extension L/K we are assuming implicitly (if it's not stated specifically) that B is a free A-module.

Let $\{x_1,\ldots,x_n\}$ and $\{y_1,\ldots,y_n\}$ be two relative integral bases for L over K. There exists $a_{pi} \in A$ such that $y_p = \Sigma_{i=1}^n a_{pi}x_i$; hence (letting tr denote the trace from L to K)

$$\begin{aligned} tr(y_p y_q) &= tr(\Sigma_{i,j=1}^n a_{pi}a_{qj}x_i x_j) \\ &= \Sigma_{i,j=1}^n a_{pi}a_{qj}tr(x_i x_j). \quad \text{Thus we have the matrix equation} \\ (tr(y_p y_q)) &= (\Sigma_{i=1}^n a_{pi}tr(x_i x_j))(a_{qj})^T \\ &= (a_{pi})(tr(x_i x_j))(a_{qj})^T. \end{aligned}$$

Therefore $d_{L/K}(y_1,\ldots,y_n) = \det(a_{ij})^2 d_{L/K}(x_1,\ldots,x_n)$. Since B is a free A-module, (a_{ij}) is invertible in A; hence $\det(a_{ij}) \in U$. We have thus shown that all relative discriminants of L over K are

congruent modulo U^2. We take advantage of this relationship in making the following definition (following Frohlich in [3]):

In case B is a free A-module the numerical discriminant of L/K is the coset of $K^{\cdot}/U^2$ generated by $d_{L/K}(x_1,\ldots,x_n)$ where $\{x_1,\ldots,x_n\}$ is any relative integral basis of L/K. The numerical discriminant of L/K is denoted by $d_{L/K}$.

Suppose now that $\{x_1,\ldots,x_n\}$ is a relative integral basis of L/K and $\{y_1,\ldots,y_n\}$ is just a basis of integers (i.e., $y_i \in B$) of L/K. Keeping the notation of the above discussion we again have $d_{L/K}(y_1,\ldots,y_n) = (\det(a_{ij}))^2\, d_{L/K}(x_1,\ldots,x_n)$.

From this equation and the facts that 1) $\det(a_{ij}) \in A$ and 2) $D_{L/K}$ is the g.c.d. of all discriminants of bases of L/K consisting of integers, we deduce that $D_{L/K} = d_{L/K}(x_1,\ldots,x_n)\,A$. This actually gives the relationship of $D_{L/K}$ to $d_{L/K}$ since $d_{L/K} = d_{L/K}(x_1,\ldots,x_n)\,U^2$. Further consideration of the equation $d_{L/K}(y_1,\ldots,y_n) = (\det(a_{ij}))^2\, d_{L/K}(x_1,\ldots,x_n)$ leads us to notice that $\{y_i\}_{i=1}^n$ is a relative integral basis if and only if the following equivalent conditions hold (let $\nu_p(x)$ be the power of p dividing xA): (a_{ij}) is invertible over A; $\det(a_{ij})$ is a unit in A; $\nu_p(d_{L/K}(y_1,\ldots,y_n)) = \nu_p(d_{L/K}(x_1,\ldots,x_n))$ for all prime K-ideals p; for all p, $\nu_p(d_{L/K}(y_1,\ldots,y_n))$ is minimal in the set $\{\nu_p(d_{L/K}(z_1,\ldots,z_n))\}$ as $\{z_1,\ldots,z_n\}$ ranges over all bases of L/K with $z_i \in B$ for all i. This criterion for determining relative integral bases will be most useful later on.

Suppose now that $\{x_1,\ldots,x_n\}$ and $\{y_1,\ldots,y_n\}$ are both arbitrary bases for L/K (here we no longer assume B is a free A-module). This time $a_{ij} \in K$ (not necessarily in A) but still we have as before

$d_{L/K}(y_1,\ldots,y_n) = (\det(a_{ij}))^2 d_{L/K}(x_1,\ldots,x_n)$. We draw from this equation the following congruence

(1) $\quad d_{L/K}(y_1,\ldots,y_n) \equiv d_{L/K}(x_1,\ldots,x_n) \bmod K^{\cdot 2}$

which we will refer to from time to time.

When the base field K is replaced by Q, the rational numbers, some changes in terminology occur. Relative integral basis becomes absolute integral basis and numerical discriminant becomes absolute discriminant. Since $U^2 = \langle 1 \rangle$ the absolute discriminant is a well defined integer; it is from this fact that the numerical discriminant (which isn't usually a number) gets its name.

It is interesting to note that if A is a P.I.D. (principal ideal domain), then the generators of $D_{L/K}$ are a certain class of $K^{\cdot}/U$ whereas $d_{L/K}$ is an element of $K^{\cdot}/U^2$. It would therefore appear that $d_{L/K}$ is more sharply defined than is $D_{L/K}$, at least in this instance. This apparent shortcoming in $D_{L/K}$ has been resolved by A. Frohlich in his creation of yet another discriminant. It is called here the idele discriminant and is defined for all extensions L/K as an element of the ideles of K modulo the squares of the unit ideles (note the analogy to $d_{L/K}$). The idele discriminant will be defined and discussed in a later section; it will be denoted $\mathcal{D}_{L/K}$.

The following terminology will be most useful in dealing with discriminants of extensions L/K. For the sake of brevity only $D_{L/K}$ is mentioned here but similar terminology will be applied in the obvious way to $d_{L/K}$ and $\mathcal{D}_{L/K}$. An extension L/K of degree ℓ is called an ℓ-extension; discriminants of ℓ-extensions will be called ℓ-discriminants. In particular, $D_{L/K}$ is an ℓ-discriminant ideal of L/K. In the special case that [L:K] = 2, $D_{L/K}$ is called a quadratic discriminant ideal.

When the ℓ-extension L/K is also cyclic, $D_{L/K}$ is called a cyclic ℓ-discriminant ideal. The expression "X is a (cyclic) ℓ-discriminant ideal of K" means that there is a (cyclic) ℓ-extension L/K for which $D_{L/K} = X$.

A prime numerical discriminant is a numerical discriminant which is represented in $K^{\cdot}/U^2$ by a power of a prime element of A (this concept applies only when A is a P.I.D.). A prime discriminant ideal of K is a discriminant ideal which is divisible by exactly one prime K-ideal.

SECTION II
UNIQUENESS IN THE FACTORIZATION AND THE CLASSICAL RESULT

The object of this thesis is to prove a generalization of a classical result concerning the prime discriminant factorization of absolute quadratic discriminants. In any generalization the question of uniqueness will inevitably arise. There are two different kinds of uniqueness that will be considered here. One involves the question of how many extensions of K generate a given discriminant. We will say that a discriminant X (be it ideal, numerical, or idele) is uniquely generated if there is only one extension L/K (of the type under consideration, e.g. cyclic ℓ-extension) such that $D_{L/K}$ (or $d_{L/K}$, or $\mathcal{D}_{L/K}$) = X. The other kind of uniqueness is the usual algebraic one, i.e., the uniqueness of the prime discriminant factors in the factorization of the given discriminant; this kind of uniqueness we call simply uniqueness of the factorization.

Theorem 1. (The Classical Result) Every absolute quadratic discriminant has a unique factorization as a product of prime absolute quadratic discriminants that are uniquely generated.

Proof: Let $L = Q(\sqrt{d})$ with d a square free integer. The following is easily established by elementary methods (see for example Samuel [9, p. 34]).

If $d \equiv 2,3 \bmod 4$, an integral basis for L/Q is $\{1,\sqrt{d}\}$; if $d \equiv 1 \bmod 4$, $\{1,(1+\sqrt{d})/2\}$ will serve as an integral basis.

The definition of discriminant of a basis applied to the case $d \equiv 2,3 \bmod 4$ yields $d_{L/Q} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$; applied to the case $d \equiv 1 \bmod 4$ it yields $d_{L/Q} = \begin{vmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{vmatrix} = d$. (These discriminants can also be calculated using the more general results of Proposition 8 that follows.)

The set of prime discriminants can easily be determined for these two cases:

If $d \equiv 2,3 \bmod 4$, $d_{L/Q}$ is a prime discriminant only if $d = \pm 2$ or $d = -1$. Therefore this case yields the prime discriminants ± 8 and -4.

If $d \equiv 1 \bmod 4$, $d_{L/Q}$ is a prime discriminant provided d is $\pm p$ where p is an odd prime. But for any odd prime p, $(-1)^{(p-1)/2} p \equiv 1 \bmod 4$. Therefore the odd prime discriminants are of the form $(-1)^{(p-1)/2} p$ where p is any odd prime.

To show that $d_{L/Q}$ can be written as a product of the prime discriminants -4, ± 8, $(-1)^{(p-1)/2} p$ (p prime), three cases are considered: (The symbol δ will be used to denote ± 1.)

1) $\underline{d \equiv 1 \bmod 4}$. Here $d_{L/Q} = d = \pm \prod_{i=1}^{m} p_i$, where the p_i are odd primes. Therefore $d_{L/Q} = \delta \prod_{i=1}^{m} (-1)^{(p_i-1)/2} p_i$; so $d \equiv \delta \bmod 4$. Thus $\delta = 1$.

2) $\underline{d \equiv 2 \bmod 4}$. It follows that $d_{L/Q} = 4d = 8\delta \prod_{i=1}^{m} (-1)^{(p_i-1)/2} p_i$. Either value of δ is permissible.

3) $\underline{d \equiv 3 \bmod 4}$. We see that $d_{L/Q} = 4d = 4\delta \prod_{i=1}^{m} (-1)^{(p_i-1)/2} p_i$ from which $d = \delta \prod_{i=1}^{m} (-1)^{(p_i-1)/2} p_i$ follows; so that $d \equiv \delta \bmod 4$. Hence $\delta = -1$.

In each instance we have found a value of δ that allows us to write $d_{L/Q}$ as a product of prime discriminants.

To deal with the question of uniqueness of the factorization suppose that $d_{L/Q}$ is an absolute quadratic discriminant with $d_{L/Q} = \prod \alpha_i$ and $d_{L/Q} = \prod \beta_i$ where the α_i, β_i are prime absolute quadratic discriminants ordered so that $\alpha_i = \pm\beta_i$ (which is possible since each α_i, β_i can itself be factored only trivially). We see that $\prod (\alpha_i/\beta_i) = 1$. If for some i, $\alpha_i = -\beta_i$, then there is an index $j \neq i$ such that $\alpha_j = -\beta_j$ also. But this would imply $\alpha_i = \pm 8$ and $\alpha_j = \pm 8$. That $\alpha_i\alpha_j \mid d_{L/Q}$ is impossible follows since $d_{L/Q} = d$ or $4d$ where d is a square free integer. Therefore $\alpha_i = \beta_i$ for all i and the factorization is unique.

That these prime discriminants are uniquely generated follows from the more general fact that, for any quadratic extension L/Q, $L = Q(\sqrt{d_{L/Q}})$.

SECTION III
DIRECTIONS FOR GENERALIZATION

In the generalizations of the classical result of Theorem 1 to be pursued in this thesis the discriminants will be calculated over a fixed field K from extensions L/K with specified Galois group G. Therefore the variables to be considered in any generalization will be the base field K, the Galois group G and the type of discriminant involved.

Ideally we would like to find a satisfactory charaterization of all fields K on which a given type of discriminant factorization holds. In fact we have acheived this goal only in the instance of $G = \sigma(2)$ (cyclic of order 2) for both the idele discriminant and the ideal discriminant. (It will be shown later that the idele discriminant encompasses conceptually both the numerical discriminant and the discriminant ideal.) For the case $G = \sigma(\ell)$ with ℓ an odd prime we will find a large class of fields K on which discriminant ideal factorization holds and we will find a large class on which it does not hold, but a characterization of such base fields K is not found. Our first generalization, which is taken up in the next section, deals with a specific example in which $G = \sigma(\ell)$, ℓ odd; K will be Q and the discriminant will be the absolute discriminant.

SECTION IV
THE FIRST GENERALIZATION

We will state in this section some well known results from algebraic number theory that will be used throughout the rest of the thesis; however, a review of p-adic fields must precede.

Let p be a rational prime. Recall that for $x \in Q^*$ $\nu_p(x)$ is the power of p dividing x. In addition we now define $\nu_p(0) = \infty$. A (non-archemedian) absolute value is defined on Q by $|x|_p = (1/p)^{\nu_p(x)}$ for $x \in Q$. (In particular $|0|_p = 0$). The field obtained by completing Q with respect to this absolute value is called the completion of Q at p and is denoted Q_p. Any finite extension of Q_p (viewed as lying in $\bar{Q}_p$, a fixed algebraic closure of Q_p, if you will) is called a p-adic field.

To see how p-adic fields arise from algebraic number fields consider K/Q, a finite extension. For a prime K-ideal $\mathfrak{p}$ we define $\nu_{\mathfrak{p}}(x)$ to be the power of $\mathfrak{p}$ dividing xA. Suppose that $\mathfrak{p} \cap Z = pZ$ for the rational prime p. We say that " $\mathfrak{p}$ lies above p " and call $e = e(\mathfrak{p}/Q) = \nu_{\mathfrak{p}}(p)$ the absolute ramification index of $\mathfrak{p}$. An absolute value is defined on K, which extends $|\cdot|_p$ on Q, by $|x|_{\mathfrak{p}} = \left[\frac{1}{p^{(1/e)}}\right]^{\nu_{\mathfrak{p}}(x)}$ for $x \in K^*$. The completion of K with respect to $|\cdot|_{\mathfrak{p}}$ is called the completion of K at $\mathfrak{p}$ and is denoted $K_{\mathfrak{p}}$. Since $Q \subseteq K$ and since $|x|_{\mathfrak{p}} = |x|_p$ for all $x \in Q$, $K_{\mathfrak{p}}$ contains (an isomorphic copy of) Q_p. If $f = [\, A/\mathfrak{p} : Z/p \,]$, the absolute inertial degree of $\mathfrak{p}$,

then $[K_p: Q_p] = ef$. Therefore K_p is a p-adic field. K_p is called a local field because it reveals the local behavior of K at the single prime p. If $\hat{Z}_p$ is the topological closure of Z in Q_p with respect to $|\cdot|_p$ and if $\hat{A}_p$ is the topological closure of A in K_p with respect to $|\cdot|_p$, then $\hat{A}_p$ is the integral closure of $\hat{Z}_p$ in K_p. The rings $\hat{Z}_p$ and $\hat{A}_p$ are discrete valuation rings (i.e., principal ideal domains with exactly one nonzero prime ideal) and are called the integers of their respective fields. The prime ideal of $\hat{A}_p$ is $p\hat{A}_p$ and there is an isomorphism $\hat{A}_p/p\hat{A}_p \cong A/p$ (we will have a closer look at this isomorphism in §5); thus $[\hat{A}_p/p\hat{A}_p : \hat{Z}_p/p\hat{Z}_p] = f$. Also there is the relation $pA_p = (p\hat{A}_p)^e$.

Now suppose $\hat{L}/\hat{K}$ is a finite abelian extension of p-adic fields with unit groups $\hat{V}/\hat{U}$. Let $\hat{p}$ be the prime ideal of $\hat{K}$. The conductor of $\hat{L}/\hat{K}$ is the smallest power $\hat{p}^m$ of $\hat{p}$ for which $N_{\hat{L}/\hat{K}}(\hat{L}^\cdot) \supseteq \hat{U}(m)$, where $\hat{U}(m) = \{x \in \hat{U}: x \equiv 1 \bmod \hat{p}^m\}$ (we define $\hat{U}(0) = \hat{U}$); the conductor of $\hat{L}/\hat{K}$ is denoted $f_{\hat{L}/\hat{K}}$. That there exists an m for which $N(\hat{L}^\cdot) \supseteq \hat{U}(m)$ follows from these facts: 1) the sets $\hat{U}(n)$ form a neighborhood system of open sets about 1 and, hence, by translation these sets form a topology for $\hat{K}^\cdot$; 2) $N_{\hat{L}/\hat{K}}$ (the norm map) is a continuous function from $\hat{L}^\cdot \to \hat{K}^\cdot$ with respect to this topology. Keeping the notation of this discussion we have

Proposition 2. If $\hat{L}/\hat{K}$ is cyclic of prime degree ℓ then $D_{\hat{L}/\hat{K}} = (f_{\hat{L}/\hat{K}})^{\ell-1}$.

Proof: The reader is referred to Artin-Tate [1], corollary to Theorem 14 p. 135 and corollary to Theorem 18 p. 139.

It is usual to include among the local fields associated with an algebraic number field those fields obtained by completing K at its archimedian absolute values, i.e., for any imbedding σ: K $\to$ C (the complex numbers), we define, for each x $\in$ K, $|x|_\sigma = |\sigma(x)|$ where $|\cdot|$ denotes the usual absolute value on C. If σ is a complex imbedding the completion of K with respect to $|\cdot|_\sigma$, denoted K_σ, is C; otherwise K_σ = R (the real numbers). The imbeddings σ of K into C are called the infinite primes of K while the prime ideals of K are called the finite primes of K. (Since we will make statements about "primes" without regard to which type (finite or infinite) it is convenient to use v as a common symbol for both.) As with finite primes there is a concept of ramification for the infinite primes of K. Given an extension L/K, when a real infinite prime σ of K has an extension to a complex infinite prime σ' of L, σ is said to ramify in L/K.

Let L/K be any abelian extension of algebraic number fields. Let v be a prime of K (finite or infinite) for which v' is any prime of L that lies over (extends) v. If v is a real prime that ramifies in L/K we set $f_{K_{v'}/K_v} = v$; if v is infinite and not ramified in L/K then we set $f_{L_{v'}/K_v} = 1$. $f_{L_{v'}/K_v}$ has already been defined in case v is finite. The conductors $f_{L_{v'}/K_v}$ are called the local conductors of L/K. The conductor of L/K (called a global conductor) is defined to be the formal product of all local conductors of K and is denoted $f_{L/K}$. Such a product is also called a cycle of K. (Although this is a formal product we will speak of one conductor (cycle) dividing another as though the terms in the product had an algebraic significance.)

We now wish to describe those aspects of class field theory

that are used in the remainder of this thesis. We follow the idele approach of Lang in [7], as opposed to the ideal approach of Janusz in [6].

Let v be a (finite or infinite) prime of K and let U_v be defined by $U_v = \hat{A}_v^*$ if v is finite,

$= K_v^*$ if v is infinite; U_v will be called the group of units of K_v. The group of ideles of a number field K is the restricted direct product of the K_v^* with respect to the U_v, i.e., it is the multiplicative group $J_K = \{x \in \prod_v K_v^* : x_v(\text{the v-component of x}) \in U_v \text{ for all but a finite number of v}\}$ where v ranges over all primes of K. It is important to note that K^* is a subgroup of J_K via $x \to (\ldots,x,x,x,\ldots)$.

By a cycle $\mathfrak{c}$ we mean the formal product of a finite number of primes of K to powers as in $\mathfrak{c} = \prod v^{m_{\mathfrak{c}}(v)}$ where $m_{\mathfrak{c}}(v)$ is a nonnegative integer called the multiplicity of v in $\mathfrak{c}$. Assume $v|\mathfrak{c}$. For v finite $W_{\mathfrak{c}}(v) = \{a \in K_v^* : a \equiv 1 \bmod p_v^{m_{\mathfrak{c}}(v)}\}$ where p_v is the prime ideal of K_v. For v real we set $W_{\mathfrak{c}}(v) = R^+$; for v complex, $W_{\mathfrak{c}}(v) = C$. We now define $W_{\mathfrak{c}} = \prod_{v|\mathfrak{c}} W_{\mathfrak{c}}(v) \prod_{v\nmid\mathfrak{c}} U_v$, a subgroup of J_K.

Our use of the Artin Reciprocity Law, which is the central theorem of class field theory, is limited to the following:

Theorem 3. (Global Class Field Theory) Let $E_{\mathfrak{c}}$ be the maximal abelian extension of K with conductor dividing a given cycle $\mathfrak{c}$ of K. Then $\mathrm{Gal}(E_{\mathfrak{c}}/K) \cong J_K/K^*W_{\mathfrak{c}}$.

($E_{\mathfrak{c}}$ is called the ray class field with cycle $\mathfrak{c}$ and $J_K/K^*W_{\mathfrak{c}}$ is called the class group corresponding to $E_{\mathfrak{c}}$).

Theorem 4. (Local Class Field Theory)

a) Let $\hat{L}/\hat{K}$ be an abelian extension of p-adic fields. Then $\mathrm{Gal}(\hat{L}/\hat{K}) \cong \dfrac{\hat{K}^*}{N_{\hat{L}/\hat{K}}(\hat{L}^*)}$.

b) Let $\hat{K}$ be a given p-adic field. The map $\hat{L} \to N_{\hat{L}/\hat{K}}(\hat{L}^*)$ establishes an inclusion reversing bijection between the finite abelian extensions of $\hat{K}$ and the open subgroups of $\hat{K}^*$ of finite index. If $H = N_{\hat{L}/\hat{K}}(\hat{L}^*)$ we say that $\hat{L}$ is the class field belonging to H and that H is the class group belonging to $\hat{L}$.

For proofs of Theorems 3 and 4 see Lang [7, Chapters 9,10, and 11].

Let $\hat{L}/\hat{K}$ be an extension of p-adic fields with prime ideals $\hat{\mathfrak{b}}$ and $\hat{\mathfrak{p}}$ respectively. Since $\hat{L}$ has only one prime ideal it makes sense to denote $e(\hat{\mathfrak{b}}/\hat{K})$ by $e(\hat{L}/\hat{K})$ and $f(\hat{\mathfrak{b}}/\hat{K})$ by $f(\hat{L}/\hat{K})$ — which we will do. The extension $\hat{L}/\hat{K}$ is said to be tamely ramified provided $p \nmid e(\hat{L}/\hat{K})$; otherwise it is wildly ramified. When $e(\hat{L}/\hat{K}) = [\hat{L}:\hat{K}]$, $\hat{L}/\hat{K}$ is said to be totally ramified.

The following proposition will be most useful in determining the conductor of an extension $\hat{L}/\hat{K}$. Both tame and wild ramifications are dealt with.

Proposition 5: Let $\hat{K}$ be a p-adic field with unit group $\hat{U}$. Let $\hat{L}/\hat{K}$ be a cyclic ℓ-extension where ℓ is prime. Let $N = N_{\hat{L}/\hat{K}}$.

a) $\hat{L}/\hat{K}$ is unramified (i.e., $e(\hat{L}/\hat{K}) = 1$) if and only if $N(\hat{L}^*) \supseteq \hat{U}$ $(= \hat{U}(0))$.

b) $\hat{L}/\hat{K}$ is tamely ramified if and only if $N(\hat{L}^*) \supseteq \hat{U}(1)$.

c) Let $e = e(\hat{K}/Q_p)$. Let n be the smallest integer for which $\hat{U}(n) \subseteq \hat{U}(1)^p$. If $(p-1) \nmid e$ or if $(p-1) \mid e$ and $\hat{K}$ contains a primitive

p^{th} root of 1, then $n = [[ep/(p-1)]] + 1$. ($[[\cdot]]$ means "greatest integer in".) If $(p-1) \mid e$ but $\hat{K}$ does not contain a primitive p^{th} root of 1, then $n = ep/(p-1)$.

d) If L/K is wildly ramified and n is as in c), then $N(\hat{L}^{\cdot}) \supseteq \hat{U}(n)$.

Proof: a) Let Π, π be prime elements of $\hat{L}$, $\hat{K}$ respectively. Then $\hat{K}^{\cdot} \cong \langle\pi\rangle \times \hat{U}$ where $\langle\pi\rangle$ is the cyclic group generated by π. $N(\Pi) = u\pi^{f(\hat{L}/\hat{K})}$ for some $u \in \hat{U}$. Therefore if $N(\hat{L}^{\cdot}) \supseteq U$, then $[\hat{K}^{\cdot}: N(\hat{L}^{\cdot})] = f(\hat{L}/\hat{K})$ which by Theorem 4 implies $f(\hat{L}/\hat{K}) = [\hat{L}:\hat{K}]$. Thus $e(\hat{L}/\hat{K}) = 1$. (Remember that the relation $[\hat{L}:\hat{K}] = e(\hat{L}/\hat{K})f(\hat{L}/\hat{K})$ holds for all p-adic fields $\hat{L}/\hat{K}$.) On the other hand if $e(\hat{L}/\hat{K}) = 1$ then $f(\hat{L}/\hat{K}) = [\hat{K}^{\cdot}: N(\hat{L}^{\cdot})]$. But $\hat{K}/N(\hat{L}^{\cdot}) \cong \dfrac{\langle\pi\rangle \times \hat{U}}{\langle\pi^{f(\hat{L}/\hat{K})}\rangle \times (N(\hat{L}^{\cdot}) \cap \hat{U})}$. Therefore $N(\hat{L}^{\cdot}) \supseteq \hat{U}$.

b) If $\hat{L}/\hat{K}$ is unramified then the result holds by part a). Assume that $\hat{L}/\hat{K}$ is ramified. Since $[\hat{L}:\hat{K}] = e(\hat{L}/\hat{K})f(\hat{L}/\hat{K}) = \ell$, a prime, it follows that $e(\hat{L}/\hat{K}) = \ell$ and $f(\hat{L}/\hat{K}) = 1$. Therefore $\langle\pi\rangle \subseteq N(\hat{L}^{\cdot})$ and consequently $[\hat{K}^{\cdot}: N(\hat{L}^{\cdot})] = [\hat{U}: N(\hat{L}^{\cdot}) \cap \hat{U}]$. This equality will be applied after we have found values for $[\hat{U}: \hat{U}(1)]$ and $[\hat{U}(1): \hat{U}(2)]$.

Let $\hat{A}$ be the ring of integers of $\hat{K}$ and let $\hat{p}$ be the prime ideal of $\hat{K}$. The natural epimorphism $\hat{U} \to (\hat{A}/\hat{p})^{\cdot}$ has kernel $\hat{U}(1)$ giving the isomorphism $\hat{U}/\hat{U}(1) \cong (\hat{A}/\hat{p})^{\cdot}$. Moreover the additive group of $\hat{A}$ maps onto $\hat{U}(1)/\hat{U}(2)$ homomorphically via $a \to 1 + a \bmod \hat{U}(2)$ with kernel $\hat{p}$; thus $\hat{A}/\hat{p} \cong \hat{U}(1)/\hat{U}(2)$. Now $\hat{A}/\hat{p}$ is a finite extension of the field $\hat{Z}_p/p\hat{Z}_p$ of degree f, say. But as we have remarked before $\hat{Z}_p/p\hat{Z}_p \cong Z/pZ$ which results from the natural injection $Z/pA \to \hat{Z}_p/p\hat{Z}_p$ and the fact that Z is dense in $\hat{Z}_p$ with respect to the p-adic topology. Therefore

$[\hat{U}:\hat{U}(1)] = p^f-1$ and $[\hat{U}(1);\hat{U}(2)] = p^f$. These indices together with the fact that $[\hat{K}^*:N(\hat{L}^*)] = [\hat{U}:N(\hat{L}^*) \cap \hat{U}]$ implies that $N(\hat{L}^*) \geq \hat{U}(1)$ if and only if $p \nmid [\hat{K}^*:N(\hat{L}^*)]$. By Theorem 4a) $[\hat{K}^*:N(\hat{L}^*)] = [\hat{L}:\hat{K}]$. The result in b) now follows from a).

c) See Long in [8, Chapter 4, Proposition 2.11].

d) Let $G = Gal(\hat{L}/\hat{K})$. $N_{\hat{L}/\hat{K}}(x) = \prod_{\sigma \in G} \sigma(x) = x^p$ for all $x \in \hat{K}^*$ since $[\hat{L}:\hat{K}] = p$. Therefore $N_{\hat{L}/\hat{K}}(x) \geq U(1)^p$. The result in d) now follows from c).

Proposition 6. Let L/K be an extension of algebraic number fields. Let p be a prime K-ideal with prime ideal factorization in L given by $pB = \prod_{i=1}^{g} b_i^{e_i}$. Let L_{b_i}/K_p be the extensions of the completions. Then

$$D_{L/K}\, \hat{A}_p = \prod_{i=1}^{g} D_{L_{b_i}/K_p}.$$

Proof: See Long in [8, Chapter 5].

We now prove the first generalization of Theorem 1.

Theorem 7. Let ℓ be an odd prime. Every absolute cyclic ℓ-discriminant has a unique factorization as a product of prime absolute cyclic ℓ-discriminants that are uniquely generated.

Proof: The theorem will be proved first for discriminant ideals.

Let $D_{L/Q}$ be a cyclic ℓ-discriminant ideal. Suppose p is a rational prime such that $p \neq \ell$ and $p \mid D_{L/Q}$. Let b lie above p in L and further let L_b/Q_p be the extension of completions obtained by completing L at b. Let $N = N_{L_b/Q_p}$.

From Proposition 5a) and b) it follows that $F_{L_b/Q_p} = p\hat{Z}_p$.

From proposition 5a) we see that $\ell = [Q_p^*:N(L_b^*)] \mid [\hat{U}_p:\hat{U}_p(1)] = p-1$; hence $p \equiv 1 \bmod \ell$. From Propositions 2 and 6 we have $v_p(D_{L/Q}) = \ell-1$.

Suppose $\ell \mid D_{L/Q}$. Keep the same notation as above with $p = \ell$. In this case L_b/Q_ℓ is wildly ramified. Therefore from Proposition 5b) $N(L_b^*) \not\equiv \hat{U}_\ell(1)$ and from c) and d) $N(L_b^*) \supseteq \hat{U}_\ell(2)$. Therefore $F_{L_b/Q_\ell} = (\ell Z_\ell)^2$. From Propositions 2 and 6 we have $v_\ell(D_{L/Q}) = 2(\ell-1)$.

To summarize, the only primes p that can divide $D_{L/Q}$ are $p = \ell$ and $p \equiv 1 \bmod \ell$. Also to any given prime of Q there corresponds at most one prime cyclic ℓ-discriminant ideal. We need only exhibit these prime discriminant ideals and show that the fields that generate them are unique.

The ray class field to the cycle mv_∞ (v_∞ = the product of all real infinite primes) of Q is C_m, the cyclotomic field of p^{th} roots of 1. (For a proof see Lang [7, p. 209].) Since the cyclic ℓ-extensions of Q in question that have absolute discriminants $p^{\ell-1}Z$ with $p \equiv 1 \bmod \ell$ have conductors dividing pv_∞, it follows that these fields are contained in C_p (if they exist). Likewise the cyclic ℓ-extensions of Q with discriminant $\ell^{2(\ell-1)}Z$ must be contained in C_{ℓ^2} (if they exist). But C_p, $p \equiv 1 \bmod \ell$, and C_{ℓ^2} each contain exactly one cyclic ℓ-extension of Q, which, of course, must yield the required prime discriminant ideals in Q.

In what remains we will use the theorem of Stickleberger: every absolute discriminant is congruent to either 0 or 1 mod 4.

Let $d_{L/Q}$ be a cyclic ℓ-discriminant. First note that $2 \nmid d_{L/Q}$ since $2 \not\equiv 1 \bmod \ell$ and $\ell \neq 2$. Therefore $d_{L/Q} \equiv 1 \bmod 4$. So, in particular, the prime absolute cyclic ℓ-discriminants are $p^{\ell-1}$ for

$p \equiv 1 \bmod \ell$ and $\ell^{2(\ell-1)}$. But $d_{L/Q}$ differs from a product of such prime discriminants by at most a sign. Since every discriminant involved is congruent to 1 mod 4 the result follows.

SECTION V
THE CASE OF QUADRATIC DISCRIMINANT IDEALS

In this section we will characterize the algebraic number fields that have the property of prime discriminant factorization of quadratic discriminant ideals. In the next section we will show that this same characterization holds in the case of quadratic idele discriminants.

We shall prove some preliminary results, the first of which is " well known " but for which a detailed proof was not found by the author in the literature.

Proposition 8. Let $L = K(\sqrt{\alpha})$ be a quadratic extension of K with α a square free integer of K. Suppose that p is a prime K-ideal. We assume (without loss of generality)* that either $\nu_p(\alpha) = 0$ or 1. Let $\nu_p(2) = e$.

1) If $p \nmid 2$ and $p \mid \alpha$, then $\nu_p(D_{L/K}) = 1$.

2) If $p \nmid 2$ and $p \nmid \alpha$, then $\nu_p(D_{L/K}) = 0$.

3) If $p \mid 2$ and $p \mid \alpha$, then $\nu_p(D_{L/K}) = 2e + 1$.

4) If $p \mid 2$ and $p \nmid \alpha$, then $\nu_p(D_{L/K}) = 2(e - s)$, where s is the largest integer $\leq e$ for which α is a quadratic residue mod p^{2s}.

(*) Note: We will show that generality is not lost if we assume that $\nu_p(\alpha) = 0$ or 1 for all primes p that divide a fixed integral ideal b of K: Consider a particular p that divides b. Let $\alpha A = p^{r+2m}c$ where $r = 0$ or 1, m is some non-negative rational integer and $p \nmid c$. Now

we can choose an integral a in K such that a and b are relatively prime and $a = (\beta)p$ for some $\beta \in K$. (Every ideal class in the ideal class group of K contains an infinite set of prime ideals. See [7, p. 167].) Therefore $\alpha\beta^{-2m}A = pa^{2m}c$. Hence $\alpha\beta^{-2m}$ is integral, $K(\sqrt{\alpha\beta^{-2m}}) = K(\sqrt{\alpha})$, $\nu_p(\alpha\beta^{-2m}) = r$ and $\nu_{p_i}(\alpha\beta^{-2m}) = \nu_{p_i}(\alpha)$ for all $p_i \mid b$, $p_i \neq p$. If we proceed in like manner for each prime $p \mid b$ the statement at the beginning of the note will be proved. The full strength of this result, although excessive for the present application, will be needed later.

Proof: As was mentioned in Section I, $D_{L/K}$ is the greatest common divisor of the ideals $\{d_{L/K}(x_1,x_2)A$: $\{x_1,x_2\}$ is a basis for L/K and $x_1,x_2 \in B\}$. In particular $D_{L/K} \mid d_{L/K}(1,\sqrt{\alpha})A$; hence $D_{L/K} \mid 4\alpha A$. Statement 2) of the proposition follows immediately from this relation. Statement 1) follows from this relation and the fact that all discriminants of bases of L/K are congruent mod K^{*2}. (See Equation (1) of Section I).

We will next prove 4). In this proof we will find $\theta = a^{-1}(\sqrt{\alpha} - b)$ with $a,b \in K_p$ so that $\{1,\theta\}$ is a relative integral basis for $K_p(\sqrt{\alpha})/K_p$. We will apply the following useful result: If $[L:K] = n$ and if $L = K(\beta)$ with $f(X) = \text{Irred}(\beta,K)$ then $d_{L/K}(1,\beta,\beta^2,\ldots,\beta^{n-1}) = \pm N_{L/K}(f'(\beta))$. (See Long [8,Corollary 1.4 of Chapter 5]). Here L and K can be either algebraic number fields or local fields. Therefore (from the criterion for determining relative integral bases given in Section I, p. 4) it will suffice to find $a,b \in K_p$ so that $\nu_p(d(1,\theta)) = \nu_p(N_{K_p(\sqrt{\alpha})/K_p}(f'(\theta)))$ is minimal subject to the condition that f be monic with integral coefficients. We see that $f'(\theta) = 2a^{-1}\sqrt{\alpha}$ and (letting N stand for the norm from $K_p(\sqrt{\alpha})$ to K_p)

(1) $$N(f'(\theta)) = (2a^{-1})^2\alpha.$$

Therefore we seek a such that $\nu_p(a)$ is maximal (but $\leq e$) subject to the condition that f have integral coefficients. The constant term of f(X) is $(b^2-\alpha)/a^2$ which must be an integer of K_p. So if $\alpha \equiv \gamma^2 \bmod p^{2s}$ (γ is a unit and s is as in the hypothesis) we can do no better than set $b = \gamma$ and $a = \pi^s$ for some prime element π of K_p.

Checking the coefficient of X in f(X) we find $\nu_p(2b/a) = e-s \geq 0$. Thus $\{1,\theta\}$ is a relative integral basis for $K_p(\sqrt{\alpha})/K_p$, where $\theta = \pi^{-s}(\sqrt{\alpha}-\gamma)$. Therefore $\nu_p(d_{K_p(\sqrt{\alpha})/K_p}) = 2(e-s)$. Statement 4) of the proposition now follows from Proposition 6.

A very similar argument to that just given for 4) also suffices to prove 3): here note that $\nu_p(N(f'(\theta))) < 2e + 1$ only if $p \mid a$. (Consider Equation (1) above.) But then $\nu_p((b^2-\alpha)/a^2) < 0$. Since the coefficients of f(X) must be integral in K_p we conclude that $p \nmid a$. We may choose $a = 1$ and $b = 0$ since this choice will make $\nu_p(N(f'(\theta))) = 2e + 1$, which must be minimal. Hence $\{1,\sqrt{\alpha}\}$ is a relative integral basis for $K_p(\sqrt{\alpha})/K_p$ and $\nu_p(D_{L/K}) = 2e + 1$, where again we apply Proposition 6.

Corollary to Proposition 8. Let K, α, and p be as in the proposition. Let $d = d_{K_p(\sqrt{\alpha})/K_p}$. Then in cases 1) and 2) of the proposition $d = \alpha\hat{U}_p^2$. In case 4), $d = (2x^{-1})^2\alpha\hat{U}_p^2$ where $x \in \hat{A}_p^*$ and $\nu_p(x) = s$. In case 3) $d = 4\alpha U_p^2$.

Proof: Let $d(x_1,x_2) = d_{K_p(\sqrt{\alpha})/K_p}(x_1,x_2)$. The criterion given in Section I (p. 4) for determining when an integral basis is a relative integral basis applies equally well in this local case. Namely, if $\nu_p(d(\theta_1,\theta_2))$ is minimal in the set $\{\nu_p(d(\gamma_1,\gamma_2))$: $\{\gamma_1,\gamma_2\}$ is a basis for $K_p(\sqrt{\alpha})/K_p$ and $\gamma_1,\gamma_2 \in B\}$ then $\{\theta_1,\theta_2\}$ is a relative integral basis for $K_p(\sqrt{\alpha})/K_p$.

In cases 1) and 2) $d(1,\sqrt{\alpha}) \equiv \alpha \bmod U_p^2$. It therefore follows from Proposition 8 and the preceding criterion that $\{1,\sqrt{\alpha}\}$ is a relative integral basis for $K_p(\sqrt{\alpha})/K_p$ in this case.

In cases 3) and 4) integral bases were found in the proof of Proposition 8 and their discriminants can be determined from Equation (1):

case 3) $a = 1$ so $d = 4\alpha U_p^2$;

case 4) $a = \pi^s$ so $d = (2\pi^{-s})^2 \alpha U_p^2$ where π is a prime element in K_p.

A prime K-ideal p is totally ramified in L/K provided only one prime L-ideal, say b, lies over p and $e(b/K) = [L:K]$. A fact that is used in the next proposition is that the rational prime ℓ is totally ramified in C_ℓ/Q where $C_\ell = Q(\zeta_\ell)$ and ζ_ℓ is a primitive ℓ^{th} root of 1. Since $Gal(C_\ell/Q) = (Z/\ell Z)^*$ we have for a the prime C_ℓ-ideal over ℓ, that $e(a/Q) = \ell - 1$. We will also use the interesting fact that a is the principal ideal of C_ℓ generated by $1 - \zeta_\ell$. (The reader is referred to [6, Chapter I, Section 9] for proofs of claims concerning C_ℓ made in this paragraph.) Now if $K \supseteq C_\ell$ and if p is a prime K-ideal lying above ℓ it follows that $(\ell - 1) \mid e(p/Q)$ since the index of ramification is multiplicative in towers of extensions. Therefore the ideal $(\ell A)^{1/(\ell-1)}$ is defined in K.

Proposition 9. Let $K \supseteq C_\ell$, for some rational prime ℓ. Let G be the group of units in A modulo the ideal $(\ell A)^{\ell/(\ell-1)}$. Then $[G:G^\ell] = \ell^{[K:Q]}$.

Proof: For a prime K-ideal a lying over ℓ let G_a be the unit group in the quotient ring A modulo the ideal $a^{\ell e(a/Q)/(\ell-1)}$. Notice

that $G/G^{\ell} \cong \prod_{a|\ell} G_a/G_a^{\ell}$. Therefore we will have proved the proposition when we show that $[G_b:G_b^{\ell}] = \ell^{ef}$ (for fixed but arbitrary $b|\ell$ in K) where $e = e(b/Q)$ and $f = f(b/Q)$.

Let $m = e/(\ell-1)$. From this point we will transfer to the completion K_b via the ismorphism $G_b \cong \hat{U}_b/\hat{U}_b(\ell m)$. Let us prove this important isomorphism in greater generality for our future reference: Let r be any positive rational integer. Let $\hat{b} = b\hat{A}_b$. The map a mod $b^r \to$ a mod $\hat{b}^r$ induces an injective homomorphism of A/b^r into $\hat{A}_b/\hat{b}^r$. That this homomorphism is surjective follows from the fact that $\hat{A}_b$ is the closure of A in $\hat{K}_b$ under the p-adic topology defined by $|\cdot|_b$ (hence A is dense in $\hat{A}_b$). Therefore we have the isomorphism $A/b^r \cong \hat{A}_b/\hat{b}^r$. The kernel of the natural epimorphism $\hat{U}_b \to (\hat{A}_b/\hat{b}^r)^{\cdot}$ is $\hat{U}_b(r)$. Hence $(A/b^r)^{\cdot} \cong \hat{U}_b/\hat{U}_b(r)$. Returning to the case at hand, we have $G_b \cong \hat{U}_b/\hat{U}_b(\ell m)$. It follows that $\dfrac{G_b}{G_b^{\ell}} \cong \dfrac{\hat{U}_b}{\hat{U}_b(\ell m)\hat{U}_b^{\ell}}$. (For the rest of this proof we will write $\hat{U}$ for $\hat{U}_b$.)

Let $\hat{A} = \hat{A}_b$ and $\hat{b} = b\hat{A}_b$. Then the residue field $\hat{A}/\hat{b} \cong A/b$ and has order ℓ^f. A more general version of Hensel's Lemma than the one in Lemma 12 (see, for example, [8, Chapter 3, Section 2]) would imply that $\hat{A}$ contains a primitive $(\ell^f-1)^{st}$ root of 1, say ζ. The cyclic group $\langle\zeta\rangle$ is a multiplicative set of representatives of $\hat{U}/\hat{U}(1) \cong (\hat{A}/\hat{b})^{\cdot}$. Thus we arrive at the decomposition $\hat{U} = \langle\zeta\rangle \times \hat{U}(1)$. It therefore follows that

$$\frac{G_b}{G_b^{\ell}} \cong \frac{\hat{U}(1)}{\hat{U}(1)^{\ell}\hat{U}(\ell m)} \tag{1}$$

because $\langle\zeta\rangle^{\ell} = \langle\zeta\rangle$.

We will next establish the index $[\hat{U}(1):\hat{U}(1)^{\ell}]$. Consider the

composite map $\hat{U}(1) \to \hat{U}(1)^{\ell} \to \hat{U}(1)^{\ell}/\hat{U}(r)^{\ell}$ for some $r \geq 2$, where the first map is given by $x \to x^{\ell}$ and the second is the natural map. Letting ζ_{ℓ} be a primitive ℓ^{th} root of 1 in K_b we have $\dfrac{\hat{U}(1)}{\hat{U}(r)<\zeta_{\ell}>} \cong \dfrac{\hat{U}(1)^{\ell}}{\hat{U}(r)^{\ell}}$. (Let Ψ be the composite map. That $\hat{U}(r)<\zeta_{\ell}> \subseteq \ker \Psi$ is obvious. Also $\Psi(u) = 1$ implies $u^{\ell} = \alpha^{\ell}$ for some $\alpha \in \hat{U}(r)$. Therefore $u = \alpha\zeta_{\ell}^{i}$, some i.) That $\dfrac{\hat{U}(r)<\zeta_{\ell}>}{\hat{U}(r)} \cong \dfrac{<\zeta_{\ell}>}{<\zeta_{\ell}>\cap\hat{U}(r)}$ follows from the well known isomorphism: $\dfrac{AB}{B} \cong \dfrac{A}{A\cap B}$ for A, B subgroups of a given group.

Hence,

$$[\hat{U}(1):\hat{U}(r)] = [\hat{U}(1)^{\ell}:\hat{U}(r)^{\ell}][<\zeta_{\ell}>:<\zeta_{\ell}>\cap\hat{U}(r)]. \tag{2}$$

Now we will show that if r is chosen sufficiently large then $\hat{U}(r)^{\ell} = \hat{U}(r+e)$. Choose $r = 4e$. (If $\ell \neq 2$, this argument works with $r = 2e$.) Consider the following expansion:

$$(1 + x\pi^{c})^{\ell} = 1 + \ell x\pi^{c} + \binom{\ell}{2}x^{2}\pi^{2c} + \ldots + \ell x^{\ell-1}\pi^{(\ell-1)c} + x^{\ell}\pi^{\ell c}, \tag{3}$$

where $x \in \hat{U}$, c is a nonnegative rational integer and π is any prime element of K_b. Define $\nu(c) = \nu_{\pi}((1+x\pi^{c})^{\ell}-1)$. Then $\nu(c) \geq \min(c+e, c\ell)$ with equality if $e + c \neq c\ell$, i.e., $c \neq m = e/(\ell-1)$. Let $c = r$. Since $5e < 4\ell e$ it follows that $\hat{U}(r)^{\ell} \subseteq \hat{U}(r+e)$. To show that $\hat{U}(r+e) \subseteq \hat{U}(r)^{\ell}$, first notice that $4e > e\ell/(\ell-1)+1$ and so by Proposition 5c $U(r + e) \subseteq \hat{U}(1)^{\ell}$. Let $y \in \hat{U}(r+e)$. There exists c and $x \in \hat{U}$ for which $y = (1 + x\pi^{c})^{\ell}$. If $c < e/\ell-1$ then $\nu(c) = c\ell < e\ell/\ell-1 < r$ which is impossible. If $c = e/\ell-1$ then an examination of Equation (3) shows that $\nu(c) = 2c + e = 2e/(\ell-1) + e < 5e = r$ which again is impossible. If $c > e/(\ell-1)$, then $\nu(c) = c + e \geq r + e$ (since $(1 + x\pi^{c})^{\ell} \in \hat{U}(r+e)$); thus $1 + x\pi^{c} \in \hat{U}(r)$. We therefore have

$\hat{U}(r+e) \subseteq \hat{U}(r)^{\ell}$ and equality of these groups follows from the reverse containment proved above.

Let us choose r so that $r \geq 4e$ and $\zeta_{\ell} \notin \hat{U}(r)$. (Shortly we will indicate that $\zeta_{\ell} \in \hat{U}(m) \setminus \hat{U}(m+1)$; hence $r = 4e$ suffices here.) Equation (2) now becomes $[\hat{U}(1):\hat{U}(r)] = [\hat{U}(1)^{\ell}:\hat{U}(r+e)]\cdot\ell$ $= [\hat{U}(1):\hat{U}(r+e)][\hat{U}(1):\hat{U}(1)^{\ell}]^{-1}\cdot\ell$. Therefore $[\hat{U}(1):\hat{U}(1)^{\ell}]$ $= [\hat{U}(r):\hat{U}(r+e)]\cdot\ell = \ell^{ef+1}$. (Much of the argument leading to this index is from Artin via Lang [7, Chapter 2, Section 3].)

From Equation (1) and the last index we now have

$$[G_b:G_b^{\ell}] = \frac{[\hat{U}(1):\hat{U}(1)^{\ell}]}{[\hat{U}(1)^{\ell}\hat{U}(\ell m):\hat{U}(1)^{\ell}]} = \ell^{ef+1}\,[\hat{U}(1)^{\ell}\hat{U}(\ell m):\hat{U}(1)^{\ell}]^{-1}.$$

Therefore to prove the proposition it will suffice to show that $[\hat{U}(1)^{\ell}\hat{U}(\ell m):\hat{U}(1)^{\ell}] = \ell$, or, equivalently, that

$$[\hat{U}(\ell m):\hat{U}(1)^{\ell}\cap\hat{U}(\ell m)] = \ell \tag{4}$$

To this end let us first show that $\hat{U}(m)^{\ell} = \hat{U}(1)^{\ell} \cap \hat{U}(\ell m)$. Let $x \in \hat{A}$. That $v(m) := v_{\pi}((1+x\pi^{m})^{\ell}-1) \geq \min(\ell m, e+m) = \ell m$ and hence that $\hat{U}(m)^{\ell} \subseteq \hat{U}(\ell m)$ follows easily. Let $(1 + x\pi^{c})^{\ell} \in \hat{U}(\ell m)$ for some rational c and assume $x \in \hat{U}$. It follows that $v(c) \geq \ell m$. But if $c < m$, $v(c) = e + c < \ell m$. Hence $c \geq m$. We have proved that $\hat{U}(m)^{\ell} = \hat{U}(1)^{\ell} \cap \hat{U}(\ell m)$ which allows us to express Equation (4) as $[\hat{U}(\ell m):\hat{U}(m)^{\ell}] = \ell$; this is the index we must establish to complete the proof.

We have remarked that $1-\zeta_{\ell}$ generates a principal ideal in C_{ℓ} which is the prime ideal lying over ℓ with index of ramification equal to $\ell-1$. It follows that $1-\zeta_{\ell}$ is a prime element of $Q_{\ell}(\zeta_{\ell})$ and, being totally ramified in $Q_{\ell}(\zeta_{\ell})/Q_{\ell}$, must satisy $1-\zeta_{\ell} = u\pi^{e/\ell-1}$ where π is a prime element in K_b and $u \in \hat{U}$. Hence $\zeta_{\ell} \in \hat{U}(m)\setminus\hat{U}(m+1)$.

But this holds for arbitrary primitive ℓ^{th} root of 1. So $\langle\zeta_\ell\rangle \subseteq \hat{U}(m)$. Using this relation in Equation (2) with r = m we have $[\hat{U}(1)^\ell:\hat{U}(m)^\ell] = \ell^{mf-f}$. From Proposition 5c it follows that $U(1)^\ell \supseteq U(\ell m+1)$. In fact $[\hat{U}(1)^\ell:\hat{U}(\ell m+1)] = [\hat{U}(1):\hat{U}(\ell m+1)][\hat{U}(1):\hat{U}(1)^\ell]^{-1}$ $= \ell^{mf-1}$. Putting the last two indices together we have $[\hat{U}(m)^\ell:\hat{U}(\ell m+1)]$ $= \ell^{f-1}$. That $[\hat{U}(\ell m):\hat{U}(m)^\ell] = \ell$ follows immediately.

We will now give some special notation for certain important ray class fields of K. Let $K^{(1)}$ be the ray class field to the unit cycle, i.e., an empty product of primes. Let K^+ be the ray class field to the cycle ν_∞, the formal product of all real infinite primes of K. $K^{(1)}$ is called the Hilbert Class Field of K; it is the maximal abelian extension of K that is unramified over K at all primes. K^+ is called the Extended Hilbert Class Field of K; it is the maximal abelian extension of K that is unramified over K at all finite primes.

From Theorem 3, $\mathrm{Gal}(K^{(1)}/K) \cong \frac{J_K}{K^\cdot U_K}$. Let I be the group of fractional ideals of K and let P be the subgroup of I of all principal ideals of K. For an element of J_K we can write (α_ν) where $\alpha_\nu \in K_\nu^\cdot$. If ν is a finite prime we write p_ν in place of ν to stand for the prime ideal. Suppose $\alpha_\nu A_\nu = p_\nu^{r_\nu}$. We establish a homomorphism of J_K onto I by $(\alpha_\nu) \to \prod_{\nu \text{ finite}} p_\nu^{r_\nu}$. Composing this map with the natural map of I onto I/P, we arrive at a homomorphism of J_K onto I/P whose kernel is $K^\cdot U_K$. Thus $\mathrm{Gal}(K^{(1)}/K) \cong I/P$, the ideal class group of K; the order of I/P is finite and is denoted h_K.

Now notice that the natural map from $\frac{J_K}{K^\cdot W_{\nu_\infty}}$ onto $\frac{J_K}{K^\cdot U_K}$ has kernel $\frac{K^\cdot U_K}{K^\cdot W_{\nu_\infty}}$. Therefore $\mathrm{Gal}(K^+/K^{(1)}) \cong \frac{K^\cdot U_K}{K^\cdot W_{\nu_\infty}} = \frac{K^\cdot W_{\nu_\infty} U_K}{K^\cdot W_{\nu_\infty}} \cong \frac{U_K}{U_K \cap K^\cdot W_{\nu_\infty}}$,

where we use the isomorphism $\frac{AB}{B} \cong \frac{A}{A\cap B}$ for A, B subgroups of some given group G. Note also that if G is abelian and if $C \leq A$ then $A \cap BC = (A\cap B)C$. Therefore $\mathrm{Gal}(K^{(+)}/K^{(1)}) \cong \frac{U_K}{(U_K\cap K^{\cdot})W_{\nu_\infty}} \cong \frac{U_K}{UW_{\nu_\infty}}$.

For a given cycle $\mathfrak{c}$ of K let $U_{\mathfrak{c}} = \{u \in U \mid u \equiv 1 \bmod p^{m_{\mathfrak{c}}(p)}$ for p finite and $\sigma(u) > 0$ for real $\sigma \mid \mathfrak{c}\}$. In particular note that U_{ν_∞} is the set of all totally positive units of K, i.e., $\{u \in U \mid \sigma(u) > 0$ for all real $\sigma: K \to C\}$. Notice that $U_{\nu_\infty} \leq W_{\nu_\infty}$; so $[K^{+}:K^{(1)}] = [U_K:UW_{\nu_\infty}]$ $= \frac{[U_K:U_{\nu_\infty}W_{\nu_\infty}]}{[UW_{\nu_\infty}:U_{\nu_\infty}W_{\nu_\infty}]} = \frac{[U_K:W_{\nu_\infty}]}{[U:U_{\nu_\infty}]} = 2^{r_1}[U:U_{\nu_\infty}]^{-1}$ where r_1 is the number of real infinite primes of K.

Proposition 10. Let p be a prime K-ideal and let m be a non-negative rational integer. Then $\mathrm{Gal}(E_{p^m\nu_\infty}/K^{+}) \cong (A/p^m)^{\cdot}/\theta(U_{\nu_\infty})$ where $\theta: U \to (A/p^m)^{\cdot}$ is the natural map.

Proof: We will use the isomorphism $\frac{AB}{B} \cong \frac{A}{A\cap B}$ and the identity $A\cap BC = (A\cap B)C$ (where $C \leq A$) freely in this proof.

The natural map from $\frac{J_K}{K^{\cdot}W_{p^m\nu_\infty}}$ onto $\frac{J_K}{K^{\cdot}U_K}$ has kernel $\frac{K^{\cdot}U_K}{K^{\cdot}W_{p^m\nu_\infty}}$. Therefore, by class field theory, $\mathrm{Gal}(E_{p^m\nu_\infty}/K^{(1)}) \cong \frac{K^{\cdot}U_K}{K^{\cdot}W_{p^m\nu_\infty}}$ $\cong \frac{U_K}{K^{\cdot}W_{p^m\nu_\infty}\cap U_K} = \frac{U_K}{(K^{\cdot}\cap U_K)W_{p^m\nu_\infty}} = \frac{U_K}{UW_{p^m\nu_\infty}}$. The natural map of $\frac{U_K}{UW_{p^m\nu_\infty}}$ onto $\frac{U_K}{UW_{\nu_\infty}}$ has kernel $\frac{UW_{\nu_\infty}}{UW_{p^m\nu_\infty}}$. Therefore $\mathrm{Gal}(E_{p^m\nu_\infty}/K^{+}) \cong \frac{UW_{\nu_\infty}}{UW_{p^m\nu_\infty}}$ $\cong \frac{W_{\nu_\infty}}{UW_{p^m\nu_\infty}\cap W_{\nu_\infty}} = \frac{W_{\nu_\infty}}{(U\cap W_{\nu_\infty})W_{p^m\nu_\infty}} = \frac{W_{\nu_\infty}}{U_{\nu_\infty}W_{p^m\nu_\infty}} \cong \frac{\hat{U}_p}{U_{\nu_\infty}\hat{U}_p(m)}$. The last isomorphism is a consequence of the p component map applied to W_{ν_∞}.

Now consider the isomorphism $(A/p^m)^{\cdot} \cong \hat{U}_p/\hat{U}_p(m)$ where

a mod $p^m \to$ a mod $\hat{U}_p(m)$. (See the proof of Proposition 9.) Composing this last map with the natural map $\hat{U}_p/\hat{U}_p(m) \to \hat{U}_p/U_{\nu_\infty}\hat{U}_p(m)$ we arrive at the homomorphism that we shall call Ψ: $(A/p^m)^* \to \hat{U}_p/U_{\nu_\infty}\hat{U}_p(m)$. Suppose a mod p^m is in the kernel of Ψ. Then $a \in U_{\nu_\infty}\hat{U}_p(m)$ which implies that there is some $u \in U_{\nu_\infty}$ such that $a \equiv u \bmod \hat{p}^m$. Since a and $u \in A$ it follows that $a \equiv u \bmod p^m$. It is now easy to see that the sequence $U_{\nu_\infty} \xrightarrow{\Theta} (A/p^m)^* \xrightarrow{\Psi} \hat{U}_p/U_{\nu_\infty}\hat{U}_p(m) \to 1$ is exact where Θ is the homomorphism in the hypothesis. The result of the proposition is a consequence of this exact sequence and that $\mathrm{Gal}(E_{p^m\nu_\infty}/K^+) \cong \hat{U}_p/U_{\nu_\infty}\hat{U}_p(m)$.

Several of the remaining theorems will require the following lemmas:

Lemma 11. Let G be a finite cyclic group and let ℓ be a prime. If H is a subgroup of G such that $\ell \mid [G:H]$ then $H \leq G^\ell$, the subgroup of the ℓ^{th} powers in G.

Proof: Let $G = \langle\sigma\rangle$. Suppose $H = \langle\sigma^r\rangle$. Then $[G:H] = r = m\ell$. Therefore $\sigma^r = (\sigma^m)^\ell$ and $H \leq G^\ell$ follows.

The next lemma is a special case of a famous result known as Hensel's Lemma.

Lemma 12. Let ℓ be a prime. Suppose $\hat{K}$ is a finite extension of $\hat{Q}_p$ with $p \neq \ell$. Let $\hat{p}$ be the prime ideal of $\hat{K}$ and suppose $\alpha \in U$, the units of $\hat{K}$. If $\alpha \equiv \gamma^\ell \bmod \hat{p}$ for some $\gamma \in \hat{U}$ then $\alpha \in \hat{U}^\ell$.

Proof: We have $\alpha\gamma^{-\ell} \in \hat{U}(1)$, a Z_p-module. (Z_p acts exponentially; cf Long [8, p.61].) Since ℓ is a unit in Z_p the result follows.

Lemma 13. Let ℓ be any rational prime and let S be any finite set of prime K-ideals. Suppose $a \in K$ and that $a \in K_p^{\ell}$ for all prime K-ideals $p \notin S$. Then $a \in K^{\ell}$.

Proof: See Artin-Tate [1, p. 82].

Theorem 14. Let K be an algebraic number field. The following are equivalent:

1) Every quadratic discriminant ideal of K has a unique factorization as a product of prime quadratic discriminant ideals of K.

2) The class number h_K is odd and every totally positive unit is a square, i.e., $U_{\nu_\infty} = U^2$.

3) K is totally real and $[K^+:K]$ is odd.

4) The class number h_K is odd and the natural map $\Phi: U \to (A/4A)^*/(A/4A)^{*2}$ is surjective with $\ker \Phi = U^2$.

Proof: The proof of Theorem 14 will proceed as indicated:

$$1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 1).$$

1) $\Rightarrow$ 2) Let p be a prime K-ideal such that $p \nmid 2$. Let $L = K(\sqrt{\alpha})$ with $(\alpha) = pb$ where $b \neq p$ is a prime K-ideal in the inverse ideal class of p. From Proposition 8 we have $\nu_p(D_{L/K}) = 1$.

The class of any discriminant ideal is a square in the ideal class group. (The proof of this statement is deferred until Proposition 16.) So given that 1) holds it follows that p is in a square ideal class of K; but this must be true for all $p \nmid 2$. If we consider the fact that each ideal class of K contains an infinite number of prime ideals, it must be that every ideal class is a square. Hence h_K is odd.

Let $E_{p\nu_\infty}$ be the ray class field to the cycle $p\nu_\infty$ of K. Then $E_{p\nu_\infty}$ is the maximal abelian extension of K with conductor dividing $p\nu_\infty$. If $p \nmid 2$ is a prime quadratic discriminant ideal, say $D_{L/K}$, it follows from Proposition 2 that the conductor of L/K must divide $p\nu_\infty$ and hence that $L \subseteq E_{p\nu_\infty}$. By Proposition 10, $\mathrm{Gal}(E_{p\nu_\infty}/K^+) \cong (A/p)^\cdot/\theta(U_{\nu_\infty})$. Therefore $2 \mid [(A/p)^\cdot:\theta(U_{\nu_\infty})]$. But since $(A/p)^\cdot$ is cyclic (A/p is a finite field) $\frac{U_p U_{\nu_\infty}}{U_p} \subseteq \frac{U_p U^2}{U_p}$ follows from Lemma 11.

So each element of U_{ν_∞} is a quadratic residue mod p. By Lemma 12 (Hensel's Lemma) it follows that each element of U_{ν_∞} is a square in K_p. Therefore for all $p \nmid 2$, $U_{\nu_\infty} \subseteq K_p^2$. So by Lemma 13 it follows that $U_{\nu_\infty} \subseteq U^2$ since only a finite number of prime K-ideals divide 2. But $U_{\nu_\infty} \supseteq U^2$ is obvious. Therefore $U_{\nu_\infty} = U^2$.

2) $\Rightarrow$ 3) Let H be the group of all roots of unity in K. The Dirichlet Unit Theorem states that $U \cong H \times A^{r_1+r_2-1}$ where r_1 (respectively $2r_2$) is the number of real (complex) imbeddings $K \to C$. Since $[H:H^2] = 2$ it follows that $[U:U^2] = 2^{r_1+r_2}$. But we proved in the discussion preceeding Proposition 10 that $[K^+:K^{(1)}] = 2^{r_1}/[U:U_{\nu_\infty}]$. Since $U_{\nu_\infty} = U^2$, we have $r_2 = 0$ and $[K^+:K^{(1)}] = 1$. As h_K is odd by hypothesis, it follows that $[K^+:K^{(1)}]$ is odd.

3) $\Rightarrow$ 4) In case K is totally real it follows that $[U:U^2] = 2^{r_1}$. Also by Proposition 9, $[(A/4A)^\cdot:(A/4A)^{\cdot 2}] = 2^{r_1}$. We need show only that the kernel of the homomorphism Φ of the statement 4) is U^2. Certainly $U^2 \subseteq \ker \Phi$. Suppose $u \in \ker \Phi \setminus U^2$. Consider $L = K(\sqrt{u})$. By Proposition 8-4) no prime K-ideal above 2 ramifies in L/K; by Proposition 8-2) no other prime K-ideals ramify in L/K. Therefore L/K

is unramified at all finite prime K-ideals. So $L \subseteq K^+$. But $2 \nmid [K^+:K]$. This contradiction means that the relation $u \in \ker \Phi \setminus U^2$ is false so that $U^2 = \ker \Phi$.

4) $\Rightarrow$ 1) Let L/K be an arbitrary quadratic extension of K. For each $p \mid D_{L/K}$ we must produce a quadratic extension $L(p)/K$ such that $D_{L(p)/K}$ is a prime discriminant and $\nu_p(D_{L(p)/K}) = \nu_p(D_{L/K})$.

By Proposition 8 if $p \mid D_{L/K}$ but $p \nmid 2$ we must exhibit $L(p)$ such that $D_{L(p)/K} = p$. To this end let $\alpha_p A = p^{h_k}$. (Recall that h_k is the class number of K.) Since the natural map $\Phi: U \to (A/4A)^*/(A/4A)^{*2}$ is surjective, we may assume without loss of generality that α_p is a unit quadratic residue (i.e., congruent to a square) mod 4A. Therefore by Proposition 8 we may choose $L(p) = K(\sqrt{\alpha_p})$.

We now take up the case of prime K-ideals that lie over 2. Here it will be convenient to set $L = K(\sqrt{\alpha})$. In considering a particular prime $p \mid 2$ we will assume that either $\nu_p(\alpha) = 0$ or $\nu_p(\alpha) = 1$. (See the note following the statement of Proposition 8.)

Suppose first that p is a prime K-ideal lying above 2 and that $p \nmid \alpha$. Suppose $\alpha \equiv \gamma^2 \bmod p^{2s}$ for some $\gamma \in A^*$, but α is not a quadratic residue mod $p^{2(s+1)}$. (Thus we define a nonnegative integer s.) Let $e_p = e(p/Q)$. From Proposition 8 we have:

1) If $s < e_p$ then $\nu_p(D_{L/K}) = 2(e_p - s)$.

2) If $s \geq e_p$ then $\nu_p(D_{L/K}) = 0$.

We need consider only case 1). Since Φ is surjective we may choose $\alpha_p \in U$ such that

$$\alpha_p + p^{2e_p} \equiv \alpha + p^{2e_p} \bmod (A/p^{2e_p})^{*2}$$

$$\equiv 1 + p^{2e_p} \bmod (A/b^{2e_b})^{*2} \text{ for all other primes } b \mid 2 \text{ and}$$

$b \neq p$. Thus referring to Proposition 8 again, we may set $L(p) = K(\sqrt{\alpha_p})$.

Suppose now p is a prime K-ideal above 2 and $p \mid \alpha$.

Let $G = (A/4A)^{\cdot}$ and let $G' = (A/\prod_{\substack{b \mid 2 \\ b \neq p}} b^{2e_b})^{\cdot}$, where b are prime K-ideals. Let $\Psi\colon G \to G'$ be the natural map. Ψ induces $\bar{\Psi}\colon G/G^2 \to G'/G'^2$ since $\Psi(G^2) \subseteq G'^2$. But Φ is surjective and $\bar{\Psi}$ is surjective; therefore $\bar{\Psi}\circ\Phi$ is surjective. If $\alpha_p A = p^{h_K}$ we deduce exactly as was done in the case $p \nmid 2$ that α_p may be chosen such that $\alpha_p \in G'^2$. It follows from Proposition 8 that we may set $L(p) = K(\sqrt{\alpha_p})$.

SECTION VI
THE CASE OF QUADRATIC IDELE DISCRIMINANTS

Let L be a finite extension of the algebraic number field K with ring of integers B and let $\{b_i\}_{i=1}^{g}$ be the set of prime L-ideals that lie above p, a prime of K. Let L_{b_i} be the completion of L at b_i viewed as lying in the algebraic closure of K_p. Let $\hat{B}_{b_i}$ denote the ring of integers of L_{b_i}.

Let σ_i be the imbedding of L into L_{b_i}. The map given by $\ell \otimes a \to (\sigma_1(\ell)a, \sigma_2(\ell)a, \ldots, \sigma_g(\ell)a)$ provides an isomorphism of K_p-algebras $L \otimes_K K_p \cong \Pi_{i=1}^{g} L_{b_i}$. (For a proof see [8, Chapter 3, Proposition 3.12].) This same mapping leads to $B \otimes_A \hat{A}_p \cong \Pi_{i=1}^{g} \hat{B}_{b_i}$ as $\hat{A}_p$ modules. (See [8, Chapter 3, Corollary 3.13].) Thus $B \otimes_A \hat{A}_p$ is the maximal order of $L \otimes_K K_p$ (since $\hat{B}_{b_i}$ is the maximal order of L_{b_i}). The discriminant of any basis for $B \otimes_A \hat{A}_p$ as an $\hat{A}_p$-module determines a uniquely defined element of $\hat{A}_p/\hat{U}_p^2$ that is denoted $d_{L\otimes_K K_p}$ (or $d_{L\otimes K_p}$).

Since $B \otimes_A \hat{A}_p \cong \Pi_{i=1}^{g} \hat{B}_{b_i}$, it follows that

$$d_{L\otimes K_p} = \Pi_{i=1}^{g} d_{L_{b_i}/K_p}. \tag{1}$$

But from Proposition 6, $D_{L/K}\, \hat{A}_p = \Pi_{i=1}^{g} d_{L_{b_i}/K_p}\, \hat{A}_p$, so

$$d_{L\otimes K_p}\, \hat{A}_p = D_{L/K}\, \hat{A}_p. \tag{2}$$

Frohlich defines the idele discriminant of L/K, $\mathcal{D}_{L/K}$, to be the element of J_K/U_K^2 whose p^{th} component is given by $(\mathcal{D}_{L/K})_p = d_{L\otimes K_p} \in K_p$. That this actually defines an element of J_K/U_K^2 follows from the fact that $(\mathcal{D}_{L/K})_p \in \hat{U}_p / \hat{U}_p^2$ for all but a finite number of p as is seen from Equation (2) and the fact that only a finite number of primes ramify in L/K.

The natural map $\sigma\colon J_K/U_K^2 \to J_K/U_K$ takes $\mathcal{D}_{L/K}$ into $D_{L/K}$ where this ideal is viewed as an element of J_K/U_K: let $\gamma\colon J_K \to I$ be the map given in the discussion preceeding Proposition 10; $\ker \gamma = U_K$, thus $J_K/U_K \cong I$. An idele discriminant of K is said to be a prime idele discriminant of K provided its image under σ is a prime discriminant ideal of K.

For any extension L/K let $d'_{L/K}$ denote the unique element of K^*/K^{*2} with representative $d_{L/K}(x_1,\ldots,x_n)$ where $\{x_1,\ldots,x_n\}$ is any basis of L/K. (See Equation (1) of Section I.)

Proposition 15. Let L, $\{L_i\}_{i=1}^m$ be given finite extensions of K. Then $\mathcal{D}_{L/K} = \Pi_{i=1}^m \mathcal{D}_{L_i/K}$ if and only if $D_{L/K} = \Pi_{i=1}^m D_{L_i/K}$ and $d'_{L/K} = \Pi_{i=1}^m d'_{L_i/K}$.

Proof: Let δ and the δ_i be fixed but arbitrary representatives of $\mathcal{D}_{L/K}$ and the $\mathcal{D}_{L_i/K}$, respectively, in J_K. Let ω and the ω_i be fixed but arbitrary representatives of $d'_{L/K}$ and the $d'_{L_i/K}$, respectively, in K^*.

Assume $\mathcal{D}_{L/K} = \Pi_{i=1}^m \mathcal{D}_{L_i/K}$. That $D_{L/K} = \Pi_{i=1}^m D_{L/K}$ follows from properties of the homomorphism $\sigma\colon J_K/U_K^2 \to J_K/U_K$ discussed above.

Let p be a fixed but arbitrary finite prime of K. Let $\{x_i\}_{i=1}^n$ be a basis for L/K. From the theory of tensor products we know that $\{x_i \otimes 1\}$ is a basis for $L \otimes_K K_p$ over K_p. It is easy to see that

$$d_{L\otimes K_p/K_p}(x_i\otimes 1) = d_{L/K}(x_i). \tag{3}$$

Using an exactly similar argument to that used in the derivation of Equation (1) of Section I we can conclude that $d_{L\otimes K_p/K_p}(x_i\otimes 1) \equiv \delta_p \bmod K_p^{\cdot 2}$ which together with Equation (3) yields $\delta \equiv d_{L/K}(x_i) \equiv \omega \bmod J_K^2$. Thus we have (since this congruence also must hold for the pairs δ_i, ω_i) $\omega \prod_{i=1}^m \omega_i \equiv \delta \prod_{i=1}^m \delta_i \bmod J_K^2$. But $\delta \prod_{i=1}^m \delta_i \in J_K^2$, whence $\omega \prod_{i=1}^m \omega_i \in J_K^2$. By Lemma 13 we conclude that $\omega \prod_{i=1}^m \omega_i \in K^{\cdot 2}$. Therefore $d'_{L/K} = \prod_{i=1}^m d'_{L_i/K}$.

Now assume $D_{L/K} = \prod_{i=1}^m D_{L_i/K}$ and $d'_{L/K} = \prod_{i=1}^m d'_{L_i/K}$. Since $D_{L/K} = \prod_{i=1}^m D_{L_i/K}$ it follow that $\mathcal{D}_{L/K} = \gamma \prod_{i=1}^m \mathcal{D}_{L_i/K}$ where $\gamma \in U_K$. Therefore $\delta \prod_{i=1}^m \delta_i \equiv \gamma \bmod J_K^2$ and as in the first part of this proof $\delta \prod_{i=1}^m \delta_i \equiv \omega \prod_{i=1}^m \omega_i \bmod J_K^2$. But $\omega \prod_{i=1}^m \omega_i \equiv 1 \bmod J_K^2$ by hypothesis. Hence $\gamma \in U_K^2$ and it follows that $\mathcal{D}_{L/K} = \prod_{i=1}^m \mathcal{D}_{L_i/K}$.

We now prove some results of Frohlich [3] as

Propostion 16.

1) $\mathcal{D}_{L/K} \in J_K^2 K^{\cdot}/U_K^2$ for all L/K.

2) The ideal class of $D_{L/K}$ (i.e., the coset $D_{L/K}P_K$ in the group I_K/P_K) is a square.

3) If $\beta \in J_K^2 K^{\cdot}/U_K^2$ there exists at most one quadratic extension L/K such that $\mathcal{D}_{L/K} = \beta$.

Proof: 1) Let $\{x_i\}_{i=1}^n$ be a basis for L/K. In the proof of Proposition 15 we showed that $d_{L/K}(x_i) \equiv \delta \bmod J_K^2$ where $\delta U_K^2 = \mathcal{D}_{L/K}$. This yields $\mathcal{D}_{L/K} \in J_K^2 K^{\cdot}/U_K^2$.

2) Consider the isomorphism $J_K/U_K \to I$ composed with the natural map $I \to I/P$. The kernel of this composite map is $K^{\cdot}U_K/U_K$; thus $J_K/K^{\cdot}U_K \cong I/P$. As before let σ: $J_K/U_K^2 \to J_K/U_K$. It follows from 1) that $\sigma(\mathcal{D}_{L/K}) \in J_K^2K^{\cdot}/U_K$ but (identifying J_K/U_K and I) $\sigma(\mathcal{D}_{L/K}) = D_{L/K}$. Therefore the ideal class of $D_{L/K}$ is in $\frac{J_K^2K^{\cdot}}{K^{\cdot}U_K} \leq \frac{J_K}{K^{\cdot}U_K}$. The result in 2) follows.

3) Suppose L and E are both quadratic extensions of K with $\mathcal{D}_{L/K} = \mathcal{D}_{E/K}$. To show that L = E we will employ the following theorem: Let L_1, L_2 be two normal extensions of K and let S_1, S_2 be the sets of primes of K that split completely in L_1, L_2, respectively. If $S_1 \subseteq S_2$ (except possibly for a finite set) then $L_2 \subseteq L_1$. (A proof of this may be found in Janusz [6, Chapter IV, 5.5].) We will now show that a prime K-ideal p splits in L (i.e., $pB = b_1b_2$ with b_1, b_2 prime L-ideals) if and only if $d_{L\otimes K_p} = \hat{U}_p^2$:

Let $L = K(\sqrt{\alpha})$. As in Proposition 8 we may assume that $\nu_p(\alpha) = 0$ or 1. Assume p splits and b_1, b_2 are the prime L-ideals above p. We have seen that $[L_{b_i}:K_p] = e(b_i/K)f(b_i/K)$ and $\Sigma_{i=1}^2 e(b_i/K)f(b_i/K) = [L:K] = 2$. Therefore $e(b_i/K)f(b_i/K) = 1$ and $[L_{b_i}:K_p] = 1$. Hence $d_{L\otimes K_p} = 1U_p^2$ follows from Equation (1).

To prove the converse suppose that p remains prime or ramifies in L. Then $K_p(\sqrt{\alpha})$ is a quadratic extension and therefore $\alpha \notin K_p^{\cdot 2}$. (Here $K_p(\sqrt{\alpha})$ is K_p-isomorphic to the completion of L at the prime above p). From the corollary to Proposition 8 and Equation (1) it follows that $d_{L\otimes K_p} = \alpha\hat{U}_p^2$ or $\beta\alpha\hat{U}_p^2$ where β is not a unit in $\hat{K}_p$. In any case it is clear that $d_{L\otimes K_p} \neq 1\hat{U}_p^2$. Therefore if $d_{L\otimes K_p} = 1\hat{U}_p^2$ then p must split in L.

Since $\mathcal{D}_{L/K} = \mathcal{D}_{E/K}$ it follows from the preceding discussion that the prime K-ideals that split in L/K are exactly those that split in E/K. From the theorem mentioned at the beginning of the proof, we have L = E.

Theorem 17. Every quadratic idele discriminant of K has a unique factorization as a product of uniquely generated prime quadratic idele discriminants if and only if $h_K^+ = [K^+:K]$ is odd and K is totally real.

Proof: Necessity follows from properties of σ: $J_K/U_K^2 \to J_K/U_K$ and Theorem 14. Now let L/K be an arbitrary quadratic extension of K. $L = K(\sqrt{\alpha})$ for $\alpha \in A$ where we assume that $\nu_p(\alpha) = 0$ or 1 for all $p \mid D_{L/K}$. (See the note following the statement of Proposition 8.) By Theorem 14 there exist fields L(p)/K such that $L(p) = K(\sqrt{\alpha_p})$, with α_p as defined in the proof of Theorem 14 (4→1), for which $D_{L/K} = \prod_{p \mid D_{L/K}} D_{L(p)/K}$ and $D_{L(p)/K}$ is a prime quadratic discriminant ideal of K for all prime K-ideals p that divide $D_{L/K}$.

We will show that $d'_{L/K} = \prod_{p \mid D_{L/K}} d'_{L(p)/K}$. Theorem 17 (except for the uniqueness properties) will then follow from Proposition 15.

If we choose $\{1, \sqrt{\alpha_p}\}$ and $\{1, \sqrt{\alpha}\}$ as bases for L(p)/K and L/K, respectively, we see that $d_{L(p)/K}(1, \sqrt{\alpha_p}) = 4\alpha_p$ and $d_{L/K}(1, \sqrt{\alpha}) = 4\alpha$, therefore $\left(\prod_{p \mid D_{L/K}} \alpha_p\right) \cdot \alpha K^{\cdot 2} = \left(\prod_{p \mid D_{L/K}} d'_{L(p)/K}\right) \cdot d'_{L/K}$. Thus we must show that $\left(\prod_{p \mid D_{L/K}} \alpha_p\right) \cdot \alpha \in K^{\cdot 2}$.

From Equation (1) of Section I we know that $d_{L/K}(1, \sqrt{\alpha})$ is

congruent to the discriminant of any other basis of L/K modulo $K^{\cdot 2}$. Therefore $d_{L/K}(1,\sqrt{\alpha})A \equiv D_{L/K} \bmod I^2$. This holds also with L and α replaced by $L(p)$ and α_p, respectively; therefore $d_{L/K}(1,\sqrt{\alpha}) \cdot \prod_{p|D_{L/K}} d_{L(p)/K} A \equiv D_{L/K} \prod_{p|D_{L/K}} D_{L(p)/K} \bmod I^2$. Thus $(\alpha \prod_{p|D_{L/K}} \alpha_p)A \in I^2$. Since h_K is odd, $(\alpha \prod_{p|D_{L/K}} \alpha_p)A = r^2A$ for some $r \in A^{\cdot}$. Therefore there exists a unit $u \in U$ such that $\alpha \prod_{p|D_{L/K}} \alpha_p = ur^2$.

It will be convenient to distinguish four classes of prime K-ideals:

$S_0 = \{p: p|2, \nu_p(\alpha) = 1\}$

$S_1 = \{p: p|2, p\nmid\alpha, \alpha$ is not a quadratic residue mod $p^{2e_p}\}$

where $e_p = e(p/Q)$.

$S_2 = \{p: p|2\}$

$S_3 = \{p: p|D_{L/K}$ but $p\nmid 2\}$.

We now decompose the left side of the last equation to obtain $\alpha \prod_{p\in S_0} \alpha_p \prod_{p\in S_1} \alpha_p \prod_{p\in S_3} \alpha_p = ur^2$. If u is not a quadratic residue mod b^{2e_b} with $b \in S_0$ we must modify α_b in the manner that is now described. Let $u_b \in U$ be such that $u_b + b^{2e_b} \equiv u + b^{2e_b} \bmod (A/b^{2e_b})^{\cdot 2}$ and let u_b be a quadratic residue mod p^{2e_p} for all $p \in S_2$, $p \neq b$. Such a choice of u_b is possible since by Theorem 14 4) the natural map $\Phi: U \to (A/4A)^{\cdot}/(A/4A)^{\cdot 2}$ is surjective. We can now redefine $L(b)$ to be $K(\sqrt{u_b\alpha_b})$.

If on the other hand u is a quadratic residue mod b^{2e_b} set $u_b = 1$. In this way we choose a u_p for each $p \in S_0$.

We have

$$\alpha \prod_{p\in S_0} u_p^{\alpha_p} \prod_{p\in S_1} \alpha_p \prod_{p\in S_3} \alpha_p = u_0 r_1^2 \tag{4}$$

where $u_0 = u \prod_{p\in S_0} u_p$. We now show $u_0 \in U^2$. We will do this by application of Theorem 14 3) → 4) which asserts that the natural map $\Phi: U \to (A/4A)^\cdot/(A/4A)^{\cdot 2}$ has kernel U^2. Thus the proof is complete if we show that u_0 is a quadratic residue mod 4A. Clearly it will suffice (in fact, is equivalent) to show that u_0 is a quadratic residue mod p^{2e_p} for all $p|2$. This we will do by considering separately the cases $p \in S_0$, $p \in S_1$, and $p \in S_2\setminus(S_0 \cup S_1)$.

Let $b \in S_0$. Then $u_0 \equiv u \prod_{p\in S_0} u_p \bmod b^{2e_b}$ which gives $u_0 \equiv \gamma^2 u_b u \bmod b^{2e_b}$ since $\prod_{\substack{p\in S_0\\ p\neq b}} u_p \equiv \gamma^2 \bmod b^{2e_b}$ for some $\gamma \in A$ such that $b \nmid \gamma$. Because of the choice of u_b, $u_0 \equiv \gamma^2\beta^2 u^2 \bmod b^{2e_b}$ for some $\beta \in A$.

Suppose that $b \in S_1$. Let us recall that for all $p \mid D_{L/K}$ such that $p \neq b$ we chose $\alpha_p + b^{2e_b} \equiv 1 + b^{2e_b} \bmod (A/b^{2e_b})^{\cdot 2}$. Therefore there is some $\gamma \in A$ such that $b \nmid \gamma$ and $\prod_{\substack{p\mid D_{L/K}\\ p\neq b}} \alpha_p \equiv \gamma^2 \bmod b^{2e_b}$. Also recall that α_b was chosen such that $\alpha_b + b^{2e_b} \equiv \alpha + b^{2e_b} \bmod (A/b^{2e_b})^{\cdot 2}$ (and here $b \nmid \alpha$). Therefore there exists $\beta \in A$ such that $b \nmid \beta$ and $\alpha\alpha_b \equiv \alpha^2\beta^2 \bmod b^{2e_b}$. Now Equation (4) yields $\alpha^2\beta^2\gamma^2 \equiv u_0 r_1^2 \bmod b^{2e_b}$. But $b \nmid \alpha\beta\gamma$, so $b \nmid r_1$; hence u_0 is a quadratic residue mod b^{2e_b}.

Finally suppose $b \in S_0 \setminus (S_0 \cup S_1)$. Here b does not divide the left side of Equation (4) and each term is a quadratic residue mod b^{2e_b} (b does not ramify in L or L(p)). Therefore $u_0 r_1^2 \equiv s^2 \bmod b^{2e_b}$ for some $s \in A$ such that $b \nmid s$. Hence u_0 is a quadratic residue mod b^{2e_b}.

We have thus shown that u_0 is a quadratic residue mod $4A$. By Theorem 14 3) $\rightarrow$ 4) $u_0 \in U^2$. Thus $d'_{L/K} = \prod_{p|D_{L/K}} d'_{L(p)/K}$ and, by Proposition 15, $\mathcal{D}_{L/K} = \prod_{p|D_{L/K}} \mathcal{D}_{L(p)/K}$. Uniqueness of generation of all quadratic idele discriminants follows from Proposition 16. The uniqueness of the factorization is the content of the next therorm.

Theorem 18. Let K be an algebraic number field and for a prime K-ideal p let $L(p)$ and $E(p)$ denote quadratic extensions of K that are ramified at p but are unramified at all other finite primes of K. Let $\mathcal{D}_{L/K} = \prod_{p|D_{L/K}} \mathcal{D}_{L(p)/K}$ and $\mathcal{D}_{L/K} = \prod_{p|D_{L/K}} \mathcal{D}_{E(p)/K}$ be two factorizations of the idele discriminant of a quadratic extension L/K. If K is totally real and if $h_K^+ = [K^+:K]$ is odd then $\mathcal{D}_{L(p)/K} = \mathcal{D}_{E(p)/K}$ for all $p \mid D_{L/K}$ and (equivalently) $L(p) = E(p)$ for all $p \mid D_{L/K}$.

Proof: Consider for the moment that p is a fixed prime K-ideal for which an extension $L(p)/K$ exists. Let $L(p) = K(\sqrt{\alpha_p})$ where $\alpha_p \in A$. We will show that α_p can be chosen in the following way:

1) If $\nu_p(D_{L(p)/K})$ is odd then we can choose α_p such that $\alpha_p A = p^{h_K}$ and α_p is a (unit) quadratic residue mod b^{2e_b} for all $b \mid 2$ and $b \neq p$ ($e_b = e(b/Q)$).

2) If $\nu_p(D_{L(p)/K})$ is even then we can choose α_p such that $\alpha_p \in U$ and α_p is a quadratic residue mod b^{2e_b} for all $b \mid 2$ and $b \neq p$.

From Proposition 8 and the note that follows the statement of the proposition we see that, for any prime b of K, $\nu_b(D_{L(p)/K})$ is odd if and only if $\nu_b(\alpha_p)$ is odd.

Thus in case 1) $\nu_p(\alpha_p)$ is odd. Let $\alpha_p A = pC^2$ for some integral ideal C. Then $\alpha_p^h A = p^h (C^h)^2$. (Here and for the rest of this proof we let $h = h_K$.) But $C^h = cA$ for some $c \in A$. Therefore $\alpha_p^h c^{-2} A = p^h$ and, of course, $K(\sqrt{\alpha_p^h c^{-2}}) = L(p)$. From Proposition 8 it follows that $\alpha_p^h c^{-2}$ is a (unit) quadratic residue mod b^{2e_b} for all primes $b \mid 2$ and $b \neq p$ (since these b do not ramify in $L(p)/K$ by assumption).

In case 2) $\nu_b(\alpha_p)$ must be even for all primes b of K. Therefore $\alpha_p A = C^2$. But h_K is odd so $C = cA$ for some $c \in A$. Thus $\alpha_p c^{-2} A = A$. Clearly we can replace α_p with $\alpha_p c^{-2} \in U$ and again from Proposition 8 we have that $\alpha_p c^{-2}$ must be a quadratic residue mod b^{2e_b} for all $b \mid 2$, $b \neq p$.

Now let $L(p) = K(\sqrt{\alpha_p})$ and $E(p) = K(\sqrt{\beta_p})$ for each $p \mid D_{L/K}$ where we assume that the α_p, β_p have been chosen in the manner just described; that is, we will assume that $\alpha_p \in U$ and $\beta_p \in U$, or else $\alpha_p A = p^h$ and $\beta_p A = p^h$. In either case we have that α_p and β_p are unit quadratic residues mod b^{2e_b} for all $b \mid 2$ and $b \neq p$. In particular we have $\alpha_p \beta_p^{-1} \in U$ for all p.

From Proposition 15 it follows that $d_{L/K}(1,\sqrt{\alpha}) \prod_{p \mid D_{L/K}} d_{L(p)/K}(1, \sqrt{\alpha_p}) \in K^{\cdot 2}$ and likewise $d_{L/K}(1, \sqrt{\alpha}) \prod_{p \mid D_{L/K}} d_{E(p)/K}(1, \sqrt{\beta_p}) \in K^{\cdot 2}$. Thus $\prod_{p \mid D_{L/K}} \alpha_p \beta_p^{-1} \in U^2$ since $d_{L(p)/K}(1, \sqrt{\alpha_p}) = 4\alpha_p$ (and similarly for the other discriminants).

Let $w_p = \alpha_p \beta_p^{-1}$. Since α_p and β_p are unit quadratic residues mod b^{2e_b} for all $b \mid 2$ with $b \neq p$ it follows that w_p is also a unit quadratic residue mod b^{2e_b} for all $b \mid 2$ with $b \neq p$. But if we let $\prod_{p \mid D_{L/K}} w_p = v^2$ for some $v \in U$ then $w_{p_1} = (\prod_{\substack{p \mid D_{L/K} \\ p \neq p_1}} w_p^{-1}) v^2$ and so

$w_{p_1} \equiv r^2 \bmod p_1^{2e_{p_1}}$ for some $r \in K^\cdot$. We see then that w_p is a quadratic residue mod 4A for all $p \mid D_{L/K}$ and hence $w_p \in \ker \Phi$. (See Theroem 14 3) $\rightarrow$ 4)). Since $\ker \Phi = U^2$ it follows that $L(p) = E(p)$ for all p.

We close this section with a look at the relationship of $d_{L/K}$ to $\mathcal{D}_{L/K}$. Suppose that B is free as an A-module so that $d_{L/K}$ is defined. Let $\{x_i\}_{i=1}^n$ be a relative integral basis for L/K. Since the map $\sigma: J_K/U_K^2 \rightarrow J_K/U_K$ has the property $\sigma(\mathcal{D}_{L/K}) = D_{L/K}$ and since $D_{L/K} = d_{L/K}(x_i)A$ (§ I), we have $\nu_p(\delta_p) = \nu_p(d_{L/K}(x_i))$ for all p where we let $\delta_p \hat{U}_p^2 = (\mathcal{D}_{L/K})_p = d_{L \otimes K_p}$. But we also showed in Proposition 15 that $\delta_p \equiv d_{L/K}(x_i) \bmod K_p^{\cdot 2}$ for all p. Therefore $d_{L/K}(x_i)U_K^2 = \mathcal{D}_{L/K}$. Since $d_{L/K} \in A/U^2$ it may be considered as an element of J_K/U_K^2 via the imbedding of $K^\cdot \rightarrow J_K$. We have

Proposition 19. If B is free as an A-module then $d_{L/K} = \mathcal{D}_{L/K}$.

It follows from Proposition 19 that the classical result of Theorem 1 is a special case of Theorem 17.

SECTION VII
REMARKS ON A THEOREM OF GOLDSTEIN

The purpose of this section is to show that the results of Goldstein in [4] are a special case of Theorem 17.

Goldstein has shown

Theorem G1. If K is totally real of narrow class number 1 (i.e., $h_K^+ = 1$) then every numerical quadratic discriminant in K is a product of prime numerical quadratic discriminants that are uniquely generated.

Let L/K be an arbitrary abelian extension. Denote by L^* the maximal abelian extension of K which is unramified over L at all finite prime L-ideals.

Theorem G2. Let K be totally real of narrow class number 1. Let $d_{L/K}$ be a numerical quadratic discriminant of K which is divisible by exactly t prime K-ideals. Then

]) $[L^*:L] \geq 2^{t-1}$ and

2) The factorization of $d_{L/K}$ given in Theorem G1 is unique if and only if $[L^*:L] = 2^{t-1}$.

Now Theorem G1 is an immediate consequence of Theorem 17 and Proposition 19. But Theorem 17 and Proposition 19 also imply a uniqueness of the factorization given in Theorem G1 which is independent

of $[L^*:L]$. Thus our result in Theorem 17 is seemingly at odds with Theorem G2. We will resolve this conflict by showing that the case $[L^*:L] > 2^{t-1}$ never occurs and hence that Theorem G2 is consistent with our results.

An additional result of Goldstein will be required, but first we present some facts about Galois extensions. Suppose that L/K is Galois and G = Gal(L/K). Then G acts transitively on the prime L-ideals lying above a given prime K-ideal p. [8, Chapter 1, Section 4.1] It follows immediately from this that if b_1, b_2 are prime L-ideals over p then $e(b_1/K) = e(b_2/K)$. In case L/K is Galois we will denote the common ramification index of all prime L-ideals over p by $e(p,L/K)$.

Proposition G3. Let S be the set of all finite primes of K and let r_1 be the number of real primes of K. Then

$$[L^*:L] = \frac{h_K \, 2^{r_1} \prod_{p \in S} e(p,L/K)}{[L:K]\,[U:U_{L/K}]}$$

where $U_{L/K}$ is the set of units of K that are local norms at all finite primes of K and are totally positive.

A unit u of K is a local norm at p provided $u \in N_{L_b/K_p}(L_b^*)$ where L_b is the completion of L at any prime b that lies above p. (Since L/K is abelian $N_{L_b/K_p}(L_b^*) = N_{L_{b'}/K_p}(L_{b'}^*)$ if b' is any other prime of L lying over p.) Hasse's Norm Theorem states that if L/K is cyclic then $x \in \bigcap_{p \text{ finite}} N_{L_b/K_p}(L_b^*)$ implies $x \in N_{L/K}(L^*)$. Thus in the cyclic case $\bigcap_{p \text{ finite}} N_{L_b/K_p}(L_b^*) \cap K = N_{L/K}(L^*)$. Furthermore, $U_{L/K} = N_{L/K}(L^*) \cap U_{\nu_\infty}$.

Let us now assume the hypothesis of Theorem G2; that is, that $[L:K] = 2$ with K totally real and $h_K^+ = 1$. We have shown previously (§ 5) that $h_K^+/h_K = [K^+:K^{(1)}] = 2^{r_1}[U:U_{\nu_\infty}]^{-1}$. But here $h_K^+ = 1$, so $[U:U_{\nu_\infty}] = 2^{r_1}$. Also since K is totally real $r_2 = 0$ and therefore, by Dirichlet's unit theorem, $[U:U^2] = 2^{r_1}$. But clearly $U_{\nu_\infty} \supseteq U^2$. Therefore $U_{\nu_\infty} = U^2$ and $U_{L/K} = N_{L/K}(L^*) \cap U^2$. It follows from Proposition G3 now that $[L^*:L] = \dfrac{2^{r_1}\,2^t}{2 \cdot 2^{r_1}} = 2^{t-1}$.

Thus Goldstein's Theorem G2 is consistent with Theorem 17 and uniqueness of the factorization in Theorem G1 always holds.

Remark: Goldstein [4] also proved that the prime discriminant factors in the factorizations achieved in his results were distinct. That this kind of distinctness holds in the prime discriminant factorizations produced in this thesis is a trivial consequence of the method of our proofs. Herein we prove that given an extension L/K and a prime p that divides $D_{L/K}$ then there exists — subject to certain conditions — another extension $L(p)/K$ (of the same type as L), ramified only at p, such that $\nu_p(D_{L/K}) = \nu_p(D_{L(p)/K})$. Distinctness of the $D_{L(p)/K}$ for $p \mid D_{L/K}$ follows immediately. This illustration carries over easily to the idele discriminants.

SECTION VIII
THE CASE OF CYCLIC ℓ-DISCRIMINANT IDEALS, $\ell > 2$

We begin with a characterization of those prime K-ideals that ramify in some cyclic ℓ-extension of K with $\ell > 2$.

Proposition 20. Let K be an algebraic number field and let ℓ be an odd rational prime. Given a K-prime p, $p \nmid \ell$, there exists a cyclic ℓ-extension of K in which p ramifies if and only if $N_{K/Q}(p) \equiv 1 \bmod \ell$.

Proof: Suppose L/K is a cyclic ℓ-extension and $p \mid D_{L/K}$ is a prime K-ideal. Let b be the prime L-ideal that lies over p. Then L_b/K_p is a tamely ramified cyclic ℓ-extension. It follows from Theorem 4 that $[K_p^{\cdot} : N(L_b^{\cdot})] = \ell$. (Here we are letting N stand for N_{L_b/K_p}.) From Proposition 5b we have $\ell \mid [\hat{U}_p : \hat{U}_p(1)]$. But, as we saw in the proof of Proposition 9, $(A/p)^{\cdot} \cong \hat{U}_p/\hat{U}_p(1)$. Since $|(A/p)^{\cdot}| = N_{K/Q}(p) - 1$, it follows that $N_{K/Q}(p) \equiv 1 \bmod \ell$.

Now assume that $N_{K/Q}(p) \equiv 1 \bmod \ell$. This implies that $\ell \mid [U_p : U_p(1)]$. Therefore there exists a subgroup H of $K_p^{\cdot}$ of index ℓ which contains $\hat{U}_p(1)$ but does not contain $\hat{U}_p$. By Theorem 4, there exists an extension $\hat{L}/K_p$ such that $Gal(\hat{L}/K_p) \cong K_p^{\cdot}/H$ and $N_{\hat{L}/K_p}(\hat{L}^{\cdot}) = H$. Therefore $F_{\hat{L}/K_p} = p\hat{A}_p$, and, by Proposition 2, $D_{\hat{L}/K_p} = (pA_p)^{\ell-1}$. Therefore $\hat{L}/K_p$ is a tamely ramified cyclic ℓ-extension.

A special case of Grunwald's Theorem is needed: Let F be an

algebraic number field; q, a rational prime; and b, a prime F-ideal. Let $\hat{E}$ be a cyclic q-extension of F_b. Then there exists a cyclic q-extension E of F such that for any prime E-ideal c that lies over b, E_c is K_p-isomorphic to $\hat{E}$. (Shianghaw Wang found an error in the original Grunwald's Theorem which he pointed out in a paper of 1948. For the corrected version see [10].) Note: If $\hat{E}/F$ is ramified it follows, of course, that $b \mid D_{E/F}$, but $D_{E/F}$ is not necessarily a prime discriminant ideal.

This case of Grunwald's Theorem fits our problem exactly ($K = F$, $\ell = q$, $p = b$, $\hat{L} = \hat{E}$) and the result of the proposition follows.

In the next proposition we will refer to the natural map $\theta: U \to (A/p^m)^*$ which was introduced in Proposition 10.

Proposition 21. Let K be an algebraic number field and let ℓ be an odd rational prime. Suppose $\ell \nmid h_K$ and let p be a prime K-ideal such that $p \nmid \ell A$. There exists a cyclic ℓ-extension L/K that is ramified at p and unramified at all other finite primes if and only if $N_{K/Q}(p) \equiv 1 \bmod \ell$ and $\theta(U_{\nu_\infty}) \subseteq (A/p)^{*\ell}$. Whenever such an extension L/K exists it is unique.

Proof: Suppose that L exists. Let b be a prime L-ideal lying over p. We have from Proposition 5b (letting N stand for the norm from L_b to K_p) that $N(L_b^*) \supseteq \hat{U}_p(1)$, but $N(L_b^*) \not\supseteq \hat{U}_p$ since L_b/K_p is ramified. Therefore the conductor $F_{L_b/K_p} = p\hat{A}_p$. Since p is the only finite prime of K that ramifies in L we must have $F_{L/K} \mid p\nu_\infty$ (ν_∞ is the product of all real primes of K).

$E_{p\nu_\infty}$ is the ray class field to the cycle $p\nu_\infty$ and is the maximal

abelian extension of K with conductor dividing $p\nu_\infty$. Since $\ell \nmid h_K$ $= [K^{(1)}:K]$ and since $[K^+:K^{(1)}]$ is a power of 2 it follows from simple Galois considerations that L exists if and only if $\ell \mid [E_{p\nu_\infty}:K^+]$. (Note: $\ell \nmid h_K$ is not needed for =>.) Let $\Theta: U \to (A/p)^\cdot$ be the homomorphism given by $\Theta(u) = u \bmod p$. Then, as was shown in Proposition 10, $\ell \mid [E_{p\nu_\infty}:K^+]$ if and only if $\ell \mid [(A/p)^\cdot:\Theta(U_{\nu_\infty})]$. But $\ell \mid [(A/p)^\cdot:\Theta(U_{\nu_\infty})]$ is equivalent to $\ell \mid |(A/p)^\cdot|$ and $\Theta(U_{\nu_\infty}) \subseteq (A/p)^{\cdot\ell}$ by Lemma 11 since $(A/p)^\cdot$ is cyclic. Also because $(A/p)^\cdot$ is cyclic it follows from Proposition 10 that $\mathrm{Gal}(E_{p\nu_\infty}/K^+)$ is cyclic. Therefore the ℓ-group component of $\mathrm{Gal}(E_{p\nu_\infty}/K)$ is cyclic because $\ell \nmid [K^{(1)}:K]$ $(= h_K)$ and $[K^+:K^{(1)}]$ is a power of 2. Hence if L/K exists then it is unique.

Theorem 22. Let K be either the rational field or an imaginary quadratic field. Let ℓ be an odd rational prime. If $\ell \nmid h_K$ and if K does not contain a primitive ℓ^{th} root of 1, then for each p with $N(p) \equiv 1 \bmod \ell$ there is a unique cyclic ℓ-extension $L(p)/K$ ramified at p and unramified at all other finite primes.

Proof: Since $\zeta_\ell \notin K$, it follows from Dirichlet's unit theorem (see Theorem 14, proof of 2) => 3)) that $[U:U^\ell] = \ell^{r_1+r_2-1}$ where r_1 is the number of real primes of K and $2r_2$ is the number of complex primes. For K as given in the hypothesis either $r_1 = 1$, $r_2 = 0$, when $K = Q$, or else $r_1 = 0$, $r_2 = 1$, when $K = Q(\sqrt{d})$ for some $d < 0$. Therefore for any such K we have $U = U^\ell$. In particular it follows that $\Theta(U_{\nu_\infty}) \subseteq (A/p)^{\cdot\ell}$ ($\Theta: U \to (A/p)^\cdot$, the natural map) for all primes p of K. Application of Proposition 21 completes the proof.

We will now take up the case that was excluded from Theorem 22

by the hypothesis that $\zeta_\ell \notin K$, i.e., the case of $K = Q(\zeta_3)$ and $\ell = 3$. The class number is $h_K = 1$. (Refer to [2,Tables]) Let $3A = \beta^2 A$ be the prime ideal factorization of 3 in K ($\beta = 1 - \zeta_3$). It is known that $K(\sqrt[3]{\alpha})/K$ is unramified at βA if and if only if $\alpha \equiv \gamma^3 \bmod \beta^3 A$ for some $\gamma \in A^\cdot$. (For a proof see [5, Section 39].)

Lemma 23. Let $\alpha \in A^\cdot \setminus A^{\cdot 3}$. $K(\sqrt[3]{\alpha})/K$ is ramified at βA if and only if $\alpha \equiv \pm 1 \bmod \beta^3 A$.

Proof: We will show that $(A/\beta^3 A)^\cdot \cong \sigma(2) \times \sigma(3) \times \sigma(3)$. The lemma then follows by counting the number of cubes in the abstract group on the right-hand side. (Recall $\sigma(m)$ = cyclic of order m.)

We have shown before in this thesis (e.g., see the proof of Proposition 9) that: $(A/\beta^3 A)^\cdot \cong \hat{U}/\hat{U}(3)$ where we let $\hat{U} = \hat{U}_{\beta A}$; $\hat{U}/\hat{U}(3) \cong \hat{U}/\hat{U}(1) \times \hat{U}(1)/\hat{U}(3)$; $\hat{U}/\hat{U}(1) = (A/\beta A)^\cdot$; and $\hat{U}(i)/\hat{U}(i+1) \cong A/\beta A$ for $i \geq 1$.

Since $A/\beta A \cong Z/3Z$ we will know the structure of $A/\beta^3 A$ as soon as we know the structure of $\hat{U}(1)/\hat{U}(3)$. That $\hat{U}(1)/\hat{U}(3) \cong \sigma(3) \times \sigma(3)$ will be the content of Lemma 27 which follows. Therefore $(A/\beta^3 A)^\cdot \cong \sigma(2) \times \sigma(3) \times \sigma(3)$.

It follows from elementary ramification theory and the quadratic reciprocity law that a rational prime p splits in K/Q (i.e., it has prime factorization $pA = b_1 b_2$) if and only if $p \equiv 1 \bmod 3$. (Samuel [9, Section 5.4].) For such a p with prime factorization $pA = b_1 b_2$, let $b_1 = \alpha_1 A$. Now $N_{K/Q}(\alpha_1) = \alpha_1 \sigma(\alpha_1) = \pm p$ where $\langle\sigma\rangle = \mathrm{Gal}(K/Q)$. That $N_{K/Q}(\alpha_1) = p$ follows from the next lemma.

Lemma 24. $N_{K/Q}(x)$ is positive for all $x \in A^{\cdot}$.

Proof: Here $A = Z[\zeta_3]$. Let $N = N_{K/Q}$. Let $x = a + b\sqrt{-3}$ with $a, b \in Q$. $N(a + b\sqrt{-3}) = a^2 + 3b^2 > 0$.

Proposition 25. Let p be a rational prime and let αA be a prime K-ideal lying over p. If $p \equiv 1 \bmod 3$ but $p \not\equiv 1 \bmod 9$, then βA ramifies in $K(\sqrt[3]{\alpha})/K$.

Proof: From the fact that p splits in K and from Lemma 24, we have $p = \alpha\sigma(\alpha)$ where $\langle\sigma\rangle = \mathrm{Gal}(K/Q)$. Assume that βA does not ramify in $K(\sqrt[3]{\alpha})/K$ (note that α cannot be a cube in K). Lemma 23 implies $\alpha \equiv \pm 1 \bmod \beta^3 A$. But then $\sigma(\alpha) \equiv \pm 1 \bmod \beta^3 A$. Hence $p = \alpha\sigma(\alpha) \equiv 1 \bmod \beta^3 A$ which implies that $3^{-1}(p-1) \in A$ and $3^{-1}(p-1) \equiv 0 \bmod \beta A$. It follows that $3^{-1}(p-1) \in Z$ and $3^{-1}(p-1) \equiv 0 \bmod 3$. Hence $p \equiv 1 \bmod 9$.

In the case at hand every cyclic 3-extension of K is of the form $K(\sqrt[3]{\alpha})$ for some $\alpha \in A^{\cdot}\backslash A^{\cdot 3}$. Fix one such α and set $L = K(\sqrt[3]{\alpha})$. Suppose that L/K is ramified at some prime K-ideal p but is unramified at all other finite primes. We wish to show that $L = K(\sqrt[3]{\mu})$ where $\mu A = p$. It is well known that a prime K-ideal p ramifies in L/K whenever $\nu_p(\alpha) > 0$ and $3 \nmid \nu_p(\alpha)$. (For a proof see Hecke [5, Section 39].) It follows that $\alpha A = p^r b^3$ where $r = \pm 1$. Since $h_K = 1$, $b = bA$ for some $b \in A^{\cdot}$. Hence $\alpha b^{-3} A = p^r$ and $(\alpha b^{-3})^r A = p$. Therefore we may set $\mu = (\alpha b^{-3})^r$.

It is now clear that Proposition 25 asserts that whenever p is a prime K-ideal lying over a rational prime p such that $p \equiv 1 \bmod 3$ but $p \not\equiv 1 \bmod 9$ then there does not exist a cyclic 3-extension over K

in which p is the only ramified (finite) prime. Therefore Proposition 25 provides us with ample justification for having excluded the case $K = Q(\sqrt{-3})$, $\ell = 3$ from Theorem 22.

The case of $K = Q(\sqrt{-3})$, $\ell = 3$ which we have just finished by an explicit construction is also covered, in part, by the following general theorem; however, the proof of the theorem is by an indirect argument.

Theorem 26. Let ℓ be an odd prime. The property of prime cyclic ℓ-discriminant factorization of cyclic ℓ-discriminant ideals does not hold in algebraic number fields that contain a primitive ℓ^{th} root of 1.

Proof: We need the following result: If b is a prime C_ℓ-ideal such that $b \nmid \ell$ then $N(b) \equiv 1 \bmod \ell$. (N is the absolute norm.) To see this consider the polynomial $X^\ell - 1 \bmod b$. Let B be the ring of integers of C_ℓ. Since $\zeta_\ell \in B$, $X^\ell - 1$ splits in B/b into ℓ linear factors. Since $b \nmid \ell$ each of these linear factors must be distinct. Therefore $\ell \mid |(B/b)^*|$, i.e., $N(b) \equiv 1 \bmod \ell$.

Let us assume that the factorization property in the hypothesis does hold for some $K \supseteq C_\ell$. We will look for a contradiction.

Let p be a prime K-ideal such that $p \nmid \ell A$. Since $N(p \cap C_\ell) \equiv 1 \bmod \ell$ it follows that $N(p) \equiv 1 \bmod \ell$. Hence by Proposition 20 some power of p must be a prime cyclic ℓ-discriminant. It is pointed out in the proof of Proposition 21 that the "necessary" part of that result does not require the hypothesis that $\ell \nmid h_K$. We use this fact here to conclude that $O(U_{\nu_\infty}) \subseteq (A/p)^{*\ell}$. But this means that each element of U_{ν_∞} is congruent to an ℓ^{th} power mod p.

It follows from Lemma 12 that $U_{\nu_\infty} \subseteq \hat{U}_p^{\ell}$. But this must be true for all primes $p \nmid \ell A$. Therefore by Lemma 13 $U_{\nu_\infty} \subseteq U^{\ell}$. Now $[U:U_{\nu_\infty}]$ is a power of 2, whereas $[U:U^{\ell}]$ is a power of ℓ and yet $[U:U^{\ell}] \mid [U:U_{\nu_\infty}]$. Therefore either $U = U^{\ell}$ or $\ell = 2$. If $U = U^{\ell}$, we contradict the assumption that $C_\ell \subseteq K$. If $\ell = 2$ we contradict the hypothesis that ℓ is odd.

Lemma 27. Let ℓ be an odd rational prime and let $\hat{K}$ be a ramified quadratic extension of Q_ℓ. Let $\hat{U}$ be the units of $\hat{K}$. Then $\hat{U}(1)/\hat{U}(3) \cong \sigma(\ell) \times \sigma(\ell)$. ($\sigma(\ell)$ denotes the cyclic group of order ℓ.)

Proof: Let e be the ramification index of $\hat{K}/Q_\ell = 2$. If $\ell \neq 3$ then the greatest integer in $e\ell/(\ell-1) = [[e\ell/(\ell-1)]] = 2$. If $\zeta_3 \notin \hat{K}$ and $\ell = 3$, $[[e\ell/(\ell-1)]] = 3$. We have from Proposition 5c that $\hat{U}(3) \subseteq \hat{U}(1)^{\ell}$ in all of the cases mentioned. If $\zeta_3 \in \hat{K}$ and $\ell = 3$, we conclude from Proposition 5c that $\hat{U}(3) \not\subseteq \hat{U}(1)^{\ell}$ but $\hat{U}(4) \subseteq \hat{U}(1)^{\ell}$.

Considering an arbitrary case again we let π be a prime element of $\hat{K}$. Let $x = 1 + \alpha\pi$ with $\alpha \in \hat{A}$. Thus $x^{\ell} = 1 + \alpha\pi + \ldots + \alpha^{\ell}\pi^{\ell} \equiv 1 \bmod \pi^3$. So in all the cases of the first paragraph we have $\hat{U}(3) \supseteq \hat{U}(1)^{\ell}$. In the cases $\ell \neq 3$ and $\ell = 3$ with $\zeta_3 \notin \hat{K}$ we conclude that $\hat{U}(3) = \hat{U}(1)^{\ell}$. If $\ell = 3$ and $\zeta_3 \in \hat{K}$ we have $\hat{U}(4) = \hat{U}(1)^{\ell}$. Thus in all cases $[\hat{U}(1)/\hat{U}(3):(\hat{U}(1)/\hat{U}(3))^{\ell}] = \ell^2$. The result follows readily. (We have used implicitly the fact that $\hat{U}(i)/\hat{U}(i+1) \cong \hat{A}/\hat{p}$ which holds for all $i \geq 1$. The proof for $i = 1$ given in the proof of Proposition 5b suffices with little change to prove the general case.)

Proposition 28. Let ℓ be an odd rational prime. Let K be either

the rational field or an imaginary quadratic field. Suppose that $\ell \nmid h_K$. Let p be a prime K-ideal such that $p \mid \ell A$. If p ramifies in a cyclic ℓ-extension L/K then there exists a cyclic ℓ-extension $L(p)$ ramified only at p among finite primes and $\nu_p(D_{L/K}) = \nu_p(D_{L(p)/K})$.

Proof: The case of K = Q is dealt with in Theorem 7 where a stronger result is obtained. So let $K = Q(\sqrt{d})$ where d is a square free negative integer. Let b be a prime L-ideal above p. We seek the conductor of L_b/K_p.

Since L_b/K_p is wildly ramified it follows from Proposition 5b that $N(L_b^*) \not\equiv U_p(1)$. ($N = N_{L_b/K_p}$.) Suppose first that ℓ is unramified in K/Q. Then $[[e\ell/(\ell-1)]] = 1$ where $e = e(K_p/Q_\ell) = 1$. From Propostion 5c we have that $\hat{U}_p(2) \subseteq \hat{U}_p(1)^\ell$. Therefore $N(L_b^*) \supseteq \hat{U}_p(2)$; so the conductor of L_b/K_p is $(p\hat{A}_p)^2$. In this case by Propositions 2 and 6, $\nu_p(D_{L/K}) = 2(\ell - 1)$.

Now suppose that ℓ is ramified in K. Let us handle as a separate case that of $K = Q(\sqrt{-3})$ and $\ell = 3$. In the proof of Lemma 27 we saw that $(N(L_b^*) \supseteq) \hat{U}(1)^3 = \hat{U}(4)$. Hence $F_{L_b/K_p} = (p\hat{A}_p)^4$ so that $\nu_p(D_{L/K}) = 4(\ell - 1)$. What is important here is that there is only one p-power cyclic 3-discriminant in K. Thus if we produce just one cyclic 3-extension $L(p)/K$ in which p is the only ramified finite prime the case of $K = Q(\sqrt{-3})$ and $\ell = 3$ is complete. In fact though we will list all such extensions since there are only 3. From the discussion of the case $K = Q(\sqrt{-3})$, $\ell = 3$ that follows Theorem 22, we know that $L(p) = K(\sqrt[3]{\alpha})$ where α is a unit of K or $\alpha A = p = (1-\zeta_3)A$. If $\alpha \in U \setminus U^3$, it follows from Theorem 3 that $(1-\zeta_3)A$ ramifies in $K(\sqrt[3]{\alpha})/K$ since $h_K = 1$.

Therefore the fields from which $L(p)$ may be chosen are: $K(\sqrt[3]{\zeta_3}) = C_9$, $K(\sqrt[3]{1-\zeta_3})$, and $K(\sqrt[3]{\zeta_3(1-\zeta_3)})$.

Suppose now that ℓ is ramified in K/Q and $\zeta_\ell \notin K$. From the proof of Lemma 27 we have $\hat{U}_p(3) = \hat{U}_p(1)^\ell$ so that $N(L_b^\cdot) \supseteq \hat{U}_p(3)$. Therefore $F_{L_b/K_p} = (p\hat{A}_p)^2$ or $(p\hat{A}_p)^3$. In the latter case $\nu_p(D_{L/K}) = 3(\ell - 1)$.

In order to conclude the proof it will suffice to exhibit cyclic ℓ-extensions L_2 and L_3 of K with conductors p^2 and p^3. In fact since $\ell \nmid h_K$ it will suffice to find $L_2 \subseteq E_{p^2\nu_\infty}$ with $[L_2:K^+] = \ell$ and $L_3 \subseteq E_{p^3\nu_\infty}$ such that $L_3 \not\subseteq E_{p^2\nu_\infty}$ and $[L_3:K^+] = \ell$. (We are using implicitly the fact that $[K^+:K] = 2^{r_1}h_K[U:U_{\nu_\infty}]^{-1}$ proved just before Proposition 10.)

Let $G_m = Gal(E_{p^m\nu_\infty}/K^+)$. By Proposition 10, $G_m \cong (A/p^m)^\cdot/\Theta(U_{\nu_\infty})$. Since we are now assuming $\zeta_\ell \notin K$, $U = \langle -1 \rangle$; it follows that $\ell \nmid [U:U_{p^m}]$; hence $\ell \nmid |\Theta(U_{\nu_\infty})|$. Let $(G)_\ell$ denote the ℓ-group component of the abelian group G. We have $(G_m)_\ell \cong ((A/p^m)^\cdot)_\ell \cong \hat{U}_p(1)/\hat{U}_p(m)$. If $m = 2$, $(G_2)_\ell \cong \sigma(\ell)$ and L_2 exists as required (uniquely so, in fact). If $m = 3$, $(G_3)_\ell \cong \sigma(\ell) \times \sigma(\ell)$ by Lemma 27. This group has $\ell + 1$ subgroups of index ℓ. Therefore ℓ of these generate fields of type L_3. (The other one is L_2.)

Theorem 29. Let K be either the rational field or an imaginary quadratic field. Let ℓ be an odd rational prime. If $\ell \nmid h_K$ and if K does not contain a primitive ℓ^{th} root of 1 then every cyclic ℓ-discriminant ideal of K has a factorization as a product of prime cyclic ℓ-discriminant ideals.

Proof: This theorem is just the composite of Proposition 20, Theorem 22, and Proposition 28.

Remark: As the proof of Proposition 28 shows there is much duplication in the fields that generate prime cyclic ℓ-discriminants that divide a power of ℓ.

BIBLIOGRAPHY

1. Artin, A. and Tate, J., Class Field Theory, Benjamin, New York, 1967.

2. Borevich, Z. I. and Shafarevich, I. R., Number Theory, Academic Press, New York, 1966.

3. Fröhlich, Albrecht, "Discriminants of Algebraic Number Fields," Math. Zeitschr., 74(1960), pp. 18-28.

4. Goldstein, Larry, "On Prime Discriminants," Nagoya Math. J., 45(1971), pp. 119-127.

5. Hecke, Erich, Vorlesungen über die theorie der algebraischen Zahlen, Chelsea, New York, 1970.

6. Janusz, Gerald, Algebraic Number Fields, Academic Press, New York, 1973.

7. Lang, Serge, Algebraic Number Theory, Addison-Wesley, Reading, 1970.

8. Long, Robert L., Algebraic Number Theory, Marcel Dekker, New York, 1977.

9. Samuel, Pierre, Algebraic Theory of Numbers, Hermann, Houghton Mifflin, Boston, 1970.

10. Wang, Shianghaw, "On Grunwald's Theorem," Ann. of Math. (2), 51(1950), pp. 471-484.

BIOGRAPHICAL SKETCH

Danny Nevin Davis

Born August 11, 1946, in Rome, Georgia, to Nevin B. and Frances L. Davis. Elementary and secondary education received in Rome and Floyd County public schools; graduated from Pepperall High School, 1964. Attended Georgia Institute of Technology, 1964-68; graduated, June 1968, with the B.S. degree in Physics. Employed at Lockheed Aircraft Corporation in the Nuclear Analysis Department, 1968-70. Attended graduate school in mathematics and worked as a teaching assistant at the University of Florida, 1971-76; obtained the M.S. degree in Mathematics, 1973. Employed as instructor in mathematics at Shorter College, Rome, Georgia, 1976 to the present.

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Mark L. Teply
Chairman
Associate Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Robert L. Long
Associate Professor of Mathematics

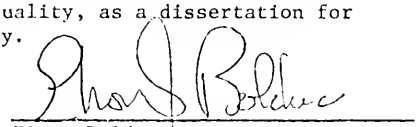
I certify that I have read this study and that in my opinion it conforms to acceptable standards f scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Beverly L. Brechner
Associate Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

Jorge Martinez
Associate Professor of Mathematics

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.



Elroy Bolduc
Associate Professor of Education

This dissertation was submitted to the Graduate Faculty of the Department of Mathematics in the College of Liberal Arts and Sciences and to the Graduate Council, and was accepted as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

December 1978

Dean, Graduate School

UNIVERSITY OF FLORIDA
3 1262 08553 2827